ESCOLA DE COMANDO E ESTADO-MAIOR DO EXÉRCITO
ESCOLA MARECHAL CASTELLO BRANCO

Maj Art HAROLDO HEITOR DE CARVALHO

A estrutura de guerra cibernética necessária para a proteção do centro de operações da Brigada de Artilharia Antiaérea: bases de uma proposta

Rio de Janeiro

2015

Maj Art HAROLDO **HEITOR** DE CARVALHO

A Estrutura de Guerra Cibernética necessária para a proteção do Centro de Operações da Brigada de Artilharia Antiaérea: bases de uma proposta

Trabalho de Conclusão de Curso apresentado à Escola de Comando e Estado-Maior do Exército, como requisito parcial para a obtenção do título de Especialista em Ciências Militares.

Orientador: Ten Cel Art Jorge Ricardo de Paula Lamellas

Rio de Janeiro
2015

C331 Carvalho, Haroldo Heitor de.

A Estrutura de Guerra Cibernética necessária para a proteção do Centro de Operações da Brigada de Artilharia Antiaérea: bases de uma proposta. / Haroldo Heitor de Carvalho. 2015.

140 f. : il ; 30cm.

Trabalho de Conclusão de Curso - Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2015.

Bibliografia: f. 133-138.

1. Guerra Cibernética. 2. Centro de Operações Antiaéreas 3. Brigada da Artilharia Antiaérea. 4. Proteção. 5 Estrutura I. Título.

CDD 355.2

Maj Art HAROLDO **HEITOR** DE CARVALHO

A Estrutura de Guerra Cibernética necessária para a proteção do Centro de Operações da Brigada de Artilharia Antiaérea: bases de uma proposta

Trabalho de Conclusão de Curso apresentado à Escola de Comando e Estado-Maior do Exército, como requisito parcial para a obtenção do título de Especialista em Ciências Militares.

Aprovado em 25 de março de 2015.

COMISSÃO AVALIADORA

_____

JORGE RICARDO DE PAULA LAMELLAS – Ten Cel Art – Presidente
Escola de Comando e Estado-Maior do Exército

_____

JOSE EUCLIDES OLIVEIRA DE ARAUJO – Maj Com – Membro
Escola de Comando e Estado-Maior do Exército

_____

HARYAN GONÇALVES DIAS – Maj Art – Membro
Escola de Comando e Estado-Maior do Exército

À minha esposa e à minha filha, minha homenagem pelo incondicional afeto e pela compreensão.

AGRADECIMENTOS

À Deus, por me conceder o dom da vida, sabedoria, proteção e saúde.

À minha família, pelo apoio, incentivo, carinho e compreensão em todos os momentos, sendo fundamentais no sucesso da conclusão deste trabalho.

Ao meu orientador, pela orientação e pela confiança demonstradas em várias oportunidades.

Aos instrutores da Escola de Comando e Estado-Maior de Exército que me auxiliaram na elaboração da pesquisa.

Aos instrutores da Escola de Artilharia de Costa e Antiaérea pelo apoio prestado a essa pesquisa.

Aos prezados amigos, que comigo realizaram o Curso de Comando e Estado-Maior, pelas colaborações ao presente trabalho monográfico e pelo convívio cordial e fraterno.

“Nunca diga às pessoas como fazer as coisas. Diga-lhes o que deve ser feito e elas o surpreenderão com sua engenhosidade**.”**
(George Patton)

RESUMO

O Exército Brasileiro (EB), alinhando-se à Estratégia Nacional de Defesa (END), está modernizando a sua Artilharia Antiaérea. A END também prioriza o desenvolvimento da defesa cibernética no Brasil. A Guerra Cibernética (G Ciber) coloca em risco a integridade de infraestruturas sensíveis, essenciais à operação e ao controle de diversos sistemas e órgãos da defesa nacional. O domínio cibernético atua nos demais domínios operacionais, onde operam as defesas antiaéreas: aeroespacial, marítimo e terrestre. A Era da Informação promoveu a incorporação das tecnologias digitais nos vetores aéreos. Isso elevou o desempenho das ameaças aéreas, dificultando a execução de defesas antiaéreas (DA Ae) nos conflitos da atualidade. Isso exige que a Artilharia Antiaérea (AAAe) disponha de modernas tecnologias de emprego militar em sua estrutura. O entendimento dos aspectos atuais do comando e controle (C^2) e da G ciber é requisito importante para o estudo dos centros de operações antiaéreas (COAAe) e das suas deficiências. Diante do elevado grau de informatização exigido por um COAAe de Bda AAAe, supõe-se que este órgão é vulnerável diante das ameaças cibernéticas. Tal hipótese exige um estudo que confirme se o referido órgão está estruturado para operar em ambiente de Guerra Cibernética. O atual processo de modernização do EB envolve a aquisição de equipamentos para os sistemas de C^2 das unidades de AAAe da Força Terrestre. O estudo dos meios de comunicações da Bda AAAe é necessário para o levantamento das vulnerabilidades frente às ações de G Ciber, pois a mesma participa da defesa aeroespacial, sendo elo na difusão de alerta e no acionamento das DA Ae contra aeronaves hostis. O objetivo geral desta pesquisa foi apresentar bases para uma proposta de estrutura de G Ciber para os COAAe da Bda AAAe do EB. Apresentou-se recomendações para que se proponha uma estrutura de G Ciber capaz de proteger o COAAe da Bda AAAe. Tais recomendações tiveram embasamento no estudo das demandas do COAAe e também no estudo dos aspectos das doutrinas de Comando e Controle e de Guerra Cibernética.

Palavras-chave: guerra cibernética; comando e controle; centro de operações antiaéreas, artilharia antiaérea, proteção; defesa aeroespacial.

ABSTRACT

The Brazilian Army (EB), aligning to the National Defense Strategy (END), has been modernizing its Antiaircraft Artillery. The END also prioritizes the development of cyber defense in Brazil. The Cyber War (G Ciber) puts at risk the integrity of critical infrastructures, essential to the operation and control of various systems and organs of national defense. The cyber domain operates in other operational areas where they operate air defenses: aerospace, marine and land. The Information Age promoted the incorporation of digital technologies in air vectors, raising the performance of air threats, hindering the mission of air defenses (DA Ae) in today's conflicts. This requires that the Antiaircraft Artillery (AAAe) has modern military use of technologies in its structure. The understanding of the current aspects of command and control (C^2) and G Ciber is an important prerequisite for the study of the anti-aircraft operations center (COAAe) and its deficiencies. Front of the high degree of computerization required by a COAAe of Brigade of AAAe , it is assumed that this body is vulnerable in the face of cyber threats. This hypothesis requires a study to confirm that this body is structured to operate in Cyber War environment. The current modernization process in the Brazilian Army involves the purchase of equipment for C^2 systems of AAAe units of the Land Force. The study of the Brigade AAAe communications resources is necessary to find the vulnerabilities facing the G Ciber activities, because it participates in the aerospace defense, being a link in the warning dissemination and activation the DA Ae against hostile aircraft. The objective of this research was to present basis for a proposed G Ciber structure for COAAe the Brazilian Army Brigade AAAe. Recommendations were introduced to propose a G Ciber structure capable of protecting the COAAe the Brigade AAAe. Such recommendations are supported in the study of the demands of COAAe and also in the study of aspects of the doctrines of command and control and Cyber War.

Keywords: cyber warfare; command and control; anti-aircraft operations center, air defense artillery, protection; aerospace defense.

LISTA DE FIGURAS

Figura 1 - Dimensões da Informação..... 30
Figura 2 - Níveis de decisão..... 36
Figura 3 - Dst Cj G Ciber no Teatro de Operações..... 37
Figura 4 - Organograma do comando e controle no TO..... 40
Figura 5 - Informações da Consciência Situacional..... 47
Figura 6 - Ciclo de *Boyd*..... 49
Figura 7 - Compatilhamento das informações na GCR..... 50
Figura 8 - Videoconferência do Comando Conjunto..... 52
Figura 9 - Comando Operacional Conjunto..... 54
Figura 10 - Célula de operações correntes do CCOA..... 55
Figura 11 - Organograma do COMDABRA, órgão central do SISDABRA..... 56
Figura 12 - Espaço Aéreo Brasileiro..... 57
Figura 13 - OCOAM..... 57
Figura 14 - Visão dos enlaces do SISCOMIS na Operação Amazônia 2012..... 62
Figura 15 - Estação Tática Transportável..... 63
Figura 16 - Rede de Telecomunicações Aeronáuticas..... 66
Figura 17 - Enlaces do SISCENDA..... 68
Figura 18 - Dispositivo URSP para RDS..... 71
Figura 19 - Console de RDS PowerSDR..... 72
Figura 20 - Console de operação do Sagitário..... 77
Figura 21 - Integração dos meios de comunicações sistema C² Cmb..... 78
Figura 22 - Visualização gráfica do terreno..... 79
Figura 23 - Sinergia das operações de informação..... 99
Figura 24 - Incidentes reportados..... 102
Figura 25 - Tipos de ataques..... 103
Figura 26 - Firewall..... 105
Figura 27 Central Unificada de Gerenciamento de Ameaças..... 109
Figura 28 - Organograma da Bda AAAe..... 116
Figura 29 - Fluxos de informações e ligações comuns do COAAe..... 118
Figura 30 - Protótipo de Equipamento RDS..... 120

Figura 31 - Shelter Orbisat COAAe S-788BR…….. 121
Figura 32 - Posto de Comando Móvel 9S737MK Ranzhir..... 121
Figura 33 - Aeronave E-99..... 122
Figura 34 - Radar SABER M200..... 123

LISTA DE QUADROS

Quadro 1 - Definição conceitual das variáveis.....25
Quadro 2 - Sistema Militar de Comando e Controle do Brasil.....53
Quadro 3 - Ligações a serem realizas por um COAAe Principal.....139

LISTA DE ABREVIATURAS E SIGLAS

AAAe	Artilharia Antiaérea
AEW&C	*Airborne Early Warning and Control*
ATN	*Aeronautical Telecommunication Network*
Bda AAAe	Brigada de Artilharia Antiaérea
Bia AAAe	Bateria de Artilharia Antiaérea
C²	Comando e Controle
CC²	Centro de Comando e Controle
CCOA	Centro Conjunto de Operações Aéreas
CCOMGEx	Centro de Comunicações e Guerra Eletrônica do Exército
CDCiber	Centro de Defesa Cibernética
CDS	Centro de Desenvolvimento de Sistemas
CIGE	Centro de Instrução de Guerra Eletrônica
CITEx	Centro Integrado de Telemática do Exército
COAAe	Centro de Operações Antiaéreas
COAAe P	Centro de Operações Antiaéreas Principal
COMDABRA	Comando de Defesa Aeroespacial Brasileiro
COMGAR	Comando-Geral de Operações Aéreas
COpM	Centro de Operações Militares
CTEx	Centro Tecnológico do Exército
D Ae	Defesa Aérea
DA Ae	Defesa Antiaérea
D Ciber	Defesa Cibernética
DCT	Departamento de Ciência e Tecnologia
DDoS	Ataque Distribuído de Negação de Serviço
DECEA	Departamento de Controle do Espaço Aéreo
Dst Cj G Ciber	Destacamento Conjunto de Guerra Cibernética
EB	Exército Brasileiro
EBNEt	Rede Corporativa Privativa do Exército
END	Estratégia Nacional de Defesa
EUA	Estados Unidos da América

ETT	Estação Tática Transportável
FAB	Força Aérea Brasileira
FAC	Força Aérea Componente
FTC	Força Terrestre Componente
GAAAe	Grupo de Artilharia Antiaérea
G Ciber	Guerra Cibernética
GCR	Guerra Centrada em Redes
GE	Guerra Eletrônica
GPS	*Global Position System*
INEW	*Integrated network-electronic warfare*
IP/MPLS	*Internet Protocol / Multiprotocol Label Switiching*
JTRS	*Joint Tactical Radio System*
MAN	*Metropolitan Area Networks*
MD	Ministério da Defesa
MPCiber	Medidas de Proteção Cibernética
MPE	Medidas de Proteção Eletrônica
NCW	*Network Centric Warfare*
NWB	*Network Warfare Battalion*
OCOAM	Órgão de Controle de Operações Aéreas Militares
OTAN	Organização do Tratado do Atlântico-Norte
RDA	Região de Defesa Aeroespacial
RDS	Rádio Definido por Software
RENASIC	Rede Nacional de Segurança da Informação e Criptografia
SAGDA	Situação Aérea Geral de Defesa Aérea
SCA	*Software Communications Architecture*
SECOS	*Secure ECCM Comunications System*
SISCEAB	Sistema de Controle do Espaço Aéreo Brasileiro
SISCENDA	Sistema de Comunicações por Enlaces Digitais da Aeronáutica
SISCOMIS	Sistema de Comunicações Militares por Satélite
SISMC²	Sistema Militar de Comando e Controle
SISTAC	Sistema Tático de Comunicações do Exército
SIVAM	Sistema de Vigilância da Amazônia
SNT	Sistema Nacional de Telecomunicações

SQL	*Structured Query Language*
STIC²	Sistemas de Tecnologia da Informação para C²
STIC3	Sistema de Tecnologia da Informação e Comunicações e Comando e Controle
TIC	Tecnologia da Informação e Comunicações
TN	Território Nacional
USRP	*Universal Software Radio Peripheral*
VPN	*Virtual Private Network*
VoIP	*Voice over Internet Protocol*
ZA	Zona de Administração
ZI	Zona do Interior

SUMÁRIO

1 **INTRODUÇÃO**..... 18
1.1 O PROBLEMA..... 20
1.2 OBJETIVOS..... 20
1.2.1 **Objetivos Específicos**..... 20
1.3 HIPÓTESE..... 21
1.4 DELIMITAÇÃO DO ESTUDO..... 21
1.5 RELEVÂNCIA DO ESTUDO..... 22
1.6 REFERENCIAL TEÓRICO..... 22
1.6.1 **Conceitos Atuais Sobre Comando e Controle**..... 22
1.6.2 **Comando e Controle na AAAe**..... 23
1.6.3 **Aspectos Doutrinários da Guerra Cibernética**..... 24
1.7 VERIFICAÇÃO DA HIPÓTESE..... 25
2 **METODOLOGIA**..... 27
3 **ASPECTOS DOUTRINÁRIOS DA GUERRA CIBERNÉTICA**..... 29
3.1 CONCEITOS GERAIS..... 29
3.1.1 **Cibernética**..... 29
3.1.2 **Espaço Cibernético ou Ciberespaço e Infraestrutura Cibernética**.... 29
3.1.3 **As Dimensões do Espaço Cibernético**..... 30
3.1.4 **Domínios Operacionais**..... 31
3.1.5 **Segurança Cibernética**..... 31
3.1.6 **Segurança da Informação e Comunicações**..... 31
3.1.7 **Defesa Cibernética**..... 32
3.1.8 **Guerra Cibernética**..... 33
3.1.9 **Sistema Militar de Defesa Cibernética (SMDC)**..... 35
3.1.10 **As Ações Cibernéticas e os Níveis de Decisão**..... 35
3.2 ASPECTOS DO NÍVEL OPERACIONAL DE DECISÃO..... 38
3.2.1 **O Destacamento Conjunto de Guerra Cibernética**..... 39

3.2.2 **O Estado-Maior Conjunto do TO e a Guerra Cibernética**..... 39
3.3 ASPECTOS DO NÍVEL TÁTICO DE DECISÃO..... 40
3.3.1 **Atuação Cibernética Tática**..... 41
3.4 A G CIBER TÁTICA, OS PRINCÍPIOS DE GUERRA E OS FUNDAMENTOS DAS OPERAÇÕES..... 41
3.5 CONSIDERAÇÕES..... 43
4 **A DOUTRINA MILITAR DE COMANDO E CONTROLE VIGENTE NO BRASIL**..... 44
4.1 OS MODERNOS ASPECTOS DO COMANDO E CONTROLE..... 44
4.1.1 **Comando e Controle (C²)**..... 44
4.1.2 **A Guerra Centrada em Redes (GCR)**..... 49
4.1.3 **O Sistema Militar de Comando e Controle (SISMC²) Brasileiro**..... 51
4.2 ASPECTOS DO C² DO SISTEMA DE DEFESA AEROESPACIA BRASILEIRO..... 54
4.2.1 **Força Aérea Componente**..... 54
4.2.2 **Processo Básico da Defesa Aeroespacial**..... 54
4.2.3 **O Comando de Defesa Aeroespacial Brasileiro (COMDABRA)**..... 55
4.3 CONSIDERAÇÕES..... 59
5 **RECURSOS DE COMANDO E CONTROLE EXISTENTES NO EXÉRCITO BRASILEIRO E NA FORÇA AÉREA BRASILEIRA**..... 61
5.1 ESTUDO DOS MEIOS DE ENLACES DE COMUNICAÇÕE CORPORATIVOS..... 61
5.1.1 **O Sistema de Comunicações Militares por Satélite (SISCOMIS)**..... 61
5.1.2 **As Redes de Voz e Dados do EB**..... 64
5.1.3 **As Redes do SISCEAB e do SISDABRA**..... 66
5.1.4 **Sistema de Comunicações por Enlaces Digitais da Aeronáutica**... 67
5.2 MEIOS DE COMUNICAÇÕES DO SISTAC DO EB..... 68
5.2.1 **O Sistema Físico**..... 68
5.2.2 **O Sistema Rádio**..... 69
5.3 ESTUDO DOS MEIOS DE COMUNICAÇÕES NA ARTILHARI ANTIAÉREA..... 73

5.3.1 **As Características do Sistema de Comunicações da AAAe**..... 73
5.4 ESTUDO DOS SISTEMAS DE APOIO À ATIVIDADE DE C²..... 75
5.4.1 **Sistemas Informatizados do SISDABRA**..... 75
5.4.2 **O Projeto C² em Combate**..... 77
5.5 CONSIDERAÇÕES..... 79
6 **O EMPREGO DAS ARMAS CIBERNÉTICAS E AS MEDIDAS DE PROTEÇÃO**..... 81
6.1 A GUERRA CIBERNÉTICA NA VISÃO DE OUTROS PAÍSES..... 81
6.1.1 **A Guerra Cibernética na República Popular da China**..... 81
6.1.2 **A Guerra Cibernética nos Estados Unidos da América**..... 85
6.1.3 **A Guerra Cibernética na Rússia**..... 88
6.2 AS AMEAÇAS CIBERNÉTICAS..... 89
6.2.1 **Estudando o Malware**..... 89
6.2.2 **Ataque Distribuído de Negação de Serviço (DDoS)**..... 94
6.2.3 **Injeção de Linguagem de Consulta Estruturada**..... 95
6.2.4 **Os atores que ameaçam o espaço cibernético**..... 95
6.3 EMPREGO DA GUERRA CIBERNÉTICA EM OPERAÇÕES DI INFORMAÇÃO..... 97
6.3.1 **A Integração das Ações Cibernéticas e de Guerra Eletrônica**..... 98
6.4 A GUERRA CIBERNÉTICA NO APOIO AO PODER AÉREO..... 99
6.4.1 **A Operação Orchard**..... 100
6.5 O ESPAÇO CIBERNÉTICO BRASILEIRO E SUAS FRAQUESAS..... 100
6.5.1 **O Espaço Cibernético Brasileiro atual**..... 101
6.5.2 **Vulnerabilidades do Espaço Cibernético Brasileiro**..... 103
6.6 MEDIDAS DE PROTEÇÃO CONTRA AMEAÇAS CIBERNÉTICAS..... 104
6.6.1 **Protegendo as Dimensões Física e Informacional**..... 105
6.6.2 **O Fator humano e a proteção da Dimensão Cognitiva**..... 110
6.7 O EXEMPLO DA FORÇA AÉREA BRASILEIRA..... 113
6.8 CONSIDERAÇÕES..... 113
7 **AS ATUAIS DEMANDAS ESTRUTURAIS DO COAAe DE BRIGADA DE AAAe**..... 116
7.1 A ATUAL ESTRUTURA DOUTRINÁRIA..... 116
7.1.1 **Comando e Controle da AAAe de Média Altura**..... 117

7.2 A ATUAL ESTRUTURA EXISTENTE PARA ATENDER AS DEMANDAS DE C² 118
7.3 AS ATUAIS NECESSIDADES DE LIGAÇÕES DO COAAe DA BRIGADA AAAe 119
7.3.1 **O COAAe P Baseado no Shelter Orbisat COAAe S-788BR** 120
7.4 REFLEXOS DAS NOVAS TECNOLOGIAS NO COAAe DE BRIGADA AAAe 121
7.5 UMA ESTRUTURA DE PROTEÇÃO CIBERNÉTICA PARA COAAe PRINCIPAL 123
7.5.1 **A base de uma proposta de recursos humanos** 123
7.5.2 **A base de uma proposta de recursos tecnológicos** 126
7.6 CONSIDERAÇÕES 127
8 **CONCLUSÃO** 128
REFERÊNCIAS 133
APÊNDICE A – Ligações a serem realizas por um COAAe Principal 139

1. INTRODUÇÃO

O Poder Militar Aeroespacial destacou-se como elemento decisivo nos principais conflitos ocorridos no mundo recentemente. Essa afirmativa vem se fundamentando desde a Operação Tempestade no Deserto, ocorrida em 1991. A campanha aérea da coalizão liderada pelos Estados Unidos da América deu inicio à operação, levando ao colapso o poderio militar iraquiano. Terminados os ataques aéreos, um dos maiores exércitos do planeta rendeu-se poucos dias após iniciadas as manobras terrestres.

Na atual Era da Informação, novas tecnologias são agregadas ao elevado desempenho dos vetores aéreos, ficando mais difícil defender-se dos mesmos a cada conflito. Nesse contexto, a defesa antiaérea torna-se elemento fundamental na política de defesa de um país. Para tanto, é mister que a estrutura da Artilharia Antiaérea (AAAe) se mantenha no "Estado da Arte", dispondo das mais recentes tecnologias em seus sistemas. Um deles é o de comando e controle, que depende de meios baseados em Tecnologia da Informação que permitam o processamento automatizado de mensagens para ser eficaz diante da rapidez do inimigo aéreo. Essa assertiva pode ser fundamentada nas abordagens dos capítulos 4, 5 e 7.

Ao estudar as demandas de comando e controle da AAAe, particularmente no que se refere ao grau informatização requerido por um COAAe de Bda AAAe, ficou notório que este órgão estará vulnerável diante das ameaças cibernéticas da atualidade.

No Brasil, a preocupação com a AAAe ficou materializada na Estratégia Nacional de Defesa (END), publicada em 2008, conforme a seguir se observa:

> "Nos centros estratégicos do País – políticos, industriais, tecnológicos e militares – a estratégia de presença do Exército concorrerá também para o objetivo de se assegurar a capacidade de defesa antiaérea, em quantidade e em qualidade, sobretudo por meio de artilharia antiaérea de média altura." (BRASIL, 2008 p. 17).

O Exército Brasileiro, alinhando-se à END, está desenvolvendo o Projeto Estratégico do Exército Defesa Antiaérea, como o objetivo de dotar a Força Terrestre de capacidade para defender as estruturas estratégicas do país contra vetores aéreos hostis, tornando as organizações militares de AAAe importantes elementos de dissuasão.

Em paralelo ao acelerado desenvolvimento dos vetores aeroespaciais, um novo campo de atuação militar vem se desenvolvendo. O ciberespaço vem ganhando relevância na atualidade ao lado das dimensões terrestre, marítima e aérea. As redes de computadores globalizaram a comunicação digital, sendo a Internet o principal elemento. Hoje, Estados e grandes instituições estão integrados a essas redes, sendo dependentes irreversíveis desses meios. Assim sendo, verifica-se que a guerra da informação tornou-se uma realidade neste campo fértil do ciberespaço, originando a guerra cibernética, cuja eficácia nos recentes conflitos armados reduziu a capacidade combativa das outras forças, aos atacar infraestruturas críticas dos Estados (FONTENELE, 2008, p. 12). Essas assertiva está apoiada no estudo do Capítulo 6.

Durante o III Seminário de Defesa Cibernética, o ministro da Defesa do Brasil, Celso Amorim (2012), afirmou:

> " A internet alterou os parâmetros de ação humana. O próprio conceito de realidade foi expandido pelo espaço digital. A cibernética emergiu como um novo domínio para a Defesa, e veio somar-se ao mar, à terra, ao ar e ao espaço. Aberto à ação humana, o domínio cibernético abre-se também ao conflito."

Infere-se, dessa forma, que todo elemento que de alguma forma interage com o espaço cibernético podem sofrer ações de Guerra Cibernética. Logo, os sistemas militares de comando e controle podem ser afetados por esses novo vetor de combate a ser estudado.

Em relação à END, o setor cibernético consta entre os três setores estratégicos considerados essenciais para a defesa nacional (BRASIL, 2008, p. 24). Atribuiu-se ao Exército Brasileiro (EB) a coordenação das atividades de Defesa Cibernética (D Ciber) no âmbito do Ministério da Defesa (MD). Esse encargo vem sendo exercido por intermédio do Centro de Defesa Cibernética, criado em 2010 como parte do Projeto Estratégico de Defesa Cibernética em andamento no EB desde 2009.

Diante da notória importância da defesa antiaérea e da defesa cibernética para a segurança do país na atualidade, estudam-se formas de estruturar e proteger o centro de operações antiaéreas de uma Brigada de AAAe de possíveis ataques cibernéticos, os quais foram apresentados nos capítulos desses trabalho.

1.1 O PROBLEMA

Os modernos equipamentos Comando e Controle (C2) e de apoio à decisão incorporam infraestruturas de telemática voltadas para suportar grandes demandas de ligações e transmissão de dados. As redes de comunicação, seja para voz, seja para imagens, são por natureza vulneráveis aos ataques cibernéticos (CARNEIRO, 2012, p. 26).

Diante disso, A END estabelece que as capacitações cibernéticas se destinarão ao mais amplo espectro de usos industriais, educativos e militares, tendo como prioridade as tecnologias de comunicação entre todos os contingentes das Forças Armadas de modo a assegurar a capacidade para atuar em rede (BRASIL, 2008, p. 24).

O atual processo de modernização do EB inclui a aquisição de meios para equipar os sistemas de comunicações e de comando e controle das unidades de Artilharia Antiaérea do EB. Assim sendo, faz-se necessário verificar se tais materiais estarão estruturados de forma a operar em ambiente de Guerra Cibernética sem que haja comprometimento da eficácia das DAAe.

Do acima exposto, abordou-se o seguinte problema:

Como pode ser estruturado o sistema de comando e controle e comunicações de uma Brigada de Artilharia Antiaérea de forma que tenha capacidade de operar frente às armas cibernéticas?

1.2 OBJETIVOS

O objetivo geral desta pesquisa foi apresentar bases para uma proposta de estrutura de Guerra Cibernética para os Centros de Operações Antiaéreas da Bda AAAe do Exército Brasileiro.

1.2.1 **Objetivos Específicos**

Nessa pesquisa foram buscados os seguintes objetivos específicos:

- Identificação dos aspectos doutrinários da Guerra Cibernética, das Comunicações e da Artilharia Antiaérea que implicam na necessidade de alterar a atual estrutura de Comando e Controle da Bda AAAe do EB.

- Identificação das ameaças empregadas na Guerra capazes de afetar os meios de comando e controle de um Bda AAAe;

- Identificação dos recursos de informação e de comunicações que poderão ser adotados para se proporcione proteção contra ataques cibernéticos ao COAAe da Bda AAAe e possibilitem a continuidade do seu funcionamento em conformidade com a doutrina vigente;

- Apresentação de propostas de soluções em recursos humanos e materiais para compor uma nova estrutura de Guerra Cibernética de um COAAe de Bda AAAe.

1.3 HIPÓTESE

O presente estudo do problema buscou-se confirmar a seguinte suposição:

O atual Centro de Operações Antiaéreas da Brigada de Artilharia Antiaérea necessita possuir uma estrutura de Guerra Cibernética para que tenha plena capacidade de operação.

1.4 DELIMITAÇÃO DO ESTUDO

A pesquisa se limita no tempo entre o período em que se iniciaram os estudos doutrinários a respeito da Guerra Cibernética no Brasil, cujo marco decisivo foi publicação da END, e a atualidade. O estudo ocorreu com base na atual doutrina militar vigente dentro do Ministério da Defesa, abordando também conhecimentos científicos específicos de segurança da informação e dos modernos sistemas de comunicações já consagrados. São abordadas as doutrinas de Guerra Cibernética que estão em formulação dentro e fora do Brasil. Junto a isso, se estudou as doutrinas de Comando e Controle e de Defesa Antiaérea, tendo como referencial teórico prioritário os manuais de campanha e os trabalhos científicos publicados nos sistemas de doutrina e de ensino superior do Exército Brasileiro.

Além disso, o estudo é centrado no sistema de comando e controle do Grupo de Artilharia Antiaérea, incluindo a literatura de operação dos equipamentos que o

compõe. Considerar-se-á o emprego desse tipo de organização militar no nível tático, ou seja, operando em proveito da missão da Força Terrestre no teatro de operações ou sob controle do Comando de Defesa Aeroespacial Brasileiro na defesa do território nacional em operações de guerra ou de conflito armado. Dessa forma, os sistemas de comunicações oriundos de outras Forças Armadas foram também estudados.

1.5 RELEVÂNCIA DO ESTUDO

Conforme relatado anteriormente, a Defesa Cibernética e a Defesa Antiaérea fazem parte de projetos estratégicos indutores da modernização do EB. São armas vitais para a proteção das estruturas estratégicas brasileiras e que demandarão pesquisas baseadas em métodos científicos. Diante disso, fica caracterizada a importância do estudo de tais assuntos para a Força Terrestre.

1.6 REFERENCIAL TEÓRICO

Os documentos apresentados na sequência serão comentados de forma que se tenha o entendimento sobre das razões que os tornam referenciais teóricos dessa pesquisa.

1.6.1 Conceitos Atuais Sobre Comando e Controle

O Manual de Doutrina Militar de Comando e Controle (MD 31-D-03), publicado pelo Ministério da Defesa em 2006, estabelece os novos conceitos a serem adotados no âmbito do Exército e nas demais forças singulares. Foram inseridos tópicos relativos a Segurança da Informação, Defesa em Redes de Computadores, recursos de Tecnologia da Informação voltados para sistemas de C2, e, principalmente, os conceitos de Guerra Centrada em Redes (GCR) e de Guerra Cibernética. Servirá de base doutrinária para o entendimento dos modernos sistemas de comunicações a serem estudados.

O referido manual assim apresenta o conceito de Guerra Centrada em Redes (GCR).

> “ GCR é uma forma de atuar na guerra com a visão específica oriunda da era da informação. Caracteriza-se pelo estabelecimento de um ambiente de compartilhamento da consciência situacional, de modo a contribuir para a obtenção da superioridade de informação e da iniciativa, mesmo que os elementos da força estejam dispersos geograficamente. A GCR enfoca o campo de batalha como uma rede integrada e dimensionada em Subredes, aumentando a velocidade e a qualidade do ciclo de C². A GCR é incremento indireto do poder de combate, aumentando a letalidade dos ataques, a rapidez nas decisões, a precisão das armas e a identificação de alvos e, também, a diminuição dos danos causados às próprias forças.” (BRASIL, 2006, p. 47).

Dentro dos conceitos de comando e controle, a referência também apresenta aspectos sobre Defesa em Redes de Computadores.

> “ A defesa nestas redes abrange a proteção dos Sistemas de Tecnologia da Informação para C² (STIC²) contra uma ação do oponente será essencial para manter a integridade da informação e a capacidade da infraestrutura de C². Compreende a proteção contra a interrupção, negação, degradação ou destruição das informações residentes em computadores e redes de computadores.” (BRASIL, 2006, p. 45)

1.6.2. Comando e Controle na AAAe

O Manual de Campanha C 44-8, Comando e Controle na Artilharia Antiérea, será o referencial básico para o estudo dos requisitos necessários para o funcionamento da estrutura de Guerra Cibernética adaptada aos COAAe de Grupo de Artilharia Antiérea, tema do trabalho. O documento citado coloca algumas condicionantes.

> “ Os centros de controle da AAAe, em qualquer escalão, devem estar em condições de estabelecer ligações interforças, procurando se beneficiar dos dados e das informações obtidas junto às estruturas de C² com as quais estejam ligados e interagem. Assim, a estrutura de C² da AAAe deverá estar em condições de suportar diferentes protocolos de comunicações e de ligar-se a redes híbridas, interligadas a diversos equipamentos e sistemas de processamento de dados.” (BRASIL, 2003, p. 1-2).

1.6.3 Aspectos Doutrinários da Guerra Cibernética

Mandarino Junior (2010), autor de Segurança e Defesa do Espaço Cibernético Brasileiro, apresenta a situação do espaço cibernético nacional e suas vulnerabilidades.

O Manual de Doutrina Militar de Comando e Controle (MD 31-D-03) assim define Guerra Cibernética (G Ciber).

> "Guerra Cibernética corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper ou destruir capacidades de C² do adversário. Compreende ações que envolvem as ferramentas de TI para desestabilizar os Sistemas de Tecnologia da Informação para C² (STIC²) do oponente e defender os próprios STIC². Abrange, essencialmente, as Operações em Redes de Computadores. A oportunidade para o emprego dessas operações ou a sua efetiva utilização será proporcional à dependência do oponente em relação à Tecnologia da Informação ." (BRASIL, 2006, p. 44)

Destaca-se a tese de doutorado denominada A Guerra Cibernética: uma proposta de elementos para formulação doutrinária no Exército Brasileiro, de autoria de João Marinonio Enke Carneiro, apresentada à Escola de Comando e Estado-Maior do Exército em 2012. Trata-se de uma referência baseada em diversas outras fontes de pesquisa, que servirá de ponto de partida para o estudo dos diversos aspectos doutrinários e pesquisas relativas à Defesa e à Guerra Cibernética. O documento descreve como está processo de estabelecimento da doutrina do MD na área de Guerra e Defesa Cibernética, propondo aspectos doutrinários a serem considerados.

Ao considerar a tendência mundial dos Estados Unidos da América (EUA), da Rússia e da China em G Ciber, a tese apresenta aspectos que devem ser inseridos na doutrina do MD e do EB e suas implicações na capacitação de recursos humanos, na aquisição de softwares e nos planos do nível operacional.

Carneiro (2012) assim apresenta a alguns aspectos doutrinários da G Ciber em outros países.

> "Para a doutrina do exército norte-americano (FM 3-13, Information Operations, 2003), a Guerra Cibernética é tratada como Operação em Redes de Computadores e dividem-se em:
> 1) Ataque a Redes de Computadores (*Computer Network Attack –CNA*);
> 2) Exploração da Rede de Computadores (*Computer Network Exploitation – CNE*); e
> 3) Defesa em Redes de Computadores (*Computer Network Defense – CND*)." (p. 36)

1.7 VERIFICAÇÃO DA HIPÓTESE

A verificação da hipótese indicou a necessidade se propor uma nova estrutura na Bda AAAe para garantir o adequado funcionamento do COAAe Principal (P) em ambiente cibernético hostil.

De acordo com o Manual para Elaboração de Projetos de Pesquisa da ECEME, ME 21-259, as variáveis constituem-se em elementos centrais da investigação e derivam da hipótese elaborada. Neste sentido, as variáveis empregadas no presente trabalho foram caracterizadas no quadro abaixo:

Quadro 1 – Definição conceitual das variáveis

<table>
<tr><th>Variável Independente</th><th>Dimensões da variável independente</th><th>Dimensões da variável dependente</th><th>Variável dependente</th></tr>
<tr><td rowspan="6">Capacidade do COAAe de Bda AAAe operar frente às armas cibernéticas</td><td>capacidade das ameaças cibernéticas e dos países que desenvolvem a G Ciber.</td><td rowspan="2">dependência do COAAe P dos sistemas apoiados em redes de computadores.</td><td rowspan="6">Estrutura do sistema de comando e controle e comunicações</td></tr>
<tr><td>emprego da G Ciber em apoio às missões aéreas de superioridade aérea e de ataque.</td></tr>
<tr><td>Necessidade de sistemas informatizados de apoio a decisão.</td><td rowspan="2">recursos humanos capazes e materiais adequados para a proteção contra ações de G Ciber.</td></tr>
<tr><td>Doutrina de G Ciber</td></tr>
<tr><td>Doutrina de Comando e Controle</td><td rowspan="2">Existência de vulnerabilidades diante das ameaças Ciber</td></tr>
<tr><td>Doutrina de emprego da AAAe</td></tr>
</table>

Fonte: o autor

A pesquisa visou apresentar bases para uma proposta de uma estrutura que permita o exercício seguro das atividades de comando e controle na Bda AAAe. Verificou-se a necessidade, salvo outro juízo, de mudanças na organização dos quadros de material e de pessoal para que exista proteção cibernética ao centro de operações antiaéreas em estudo.

2. METODOLOGIA

A concepção da pesquisa, quanto à forma de abordagem do problema, foi qualitativa. Segundo Marconi e Lakatos (2007), o estudo tem caráter qualitativo quando aprofunda pesquisas a respeito do assunto, seja por meio de livros ou artigos elaborados por estudiosos na área.

Foi aplicado como um todo o método indutivo pelo qual se levanta uma generalização a partir de situações particulares. Para os casos específicos estudados foi adotado o método hipotético-dedutivo, pelo qual a partir de premissas válidas, obteve-se a hipótese a qual foi confirmada.

No que se refere ao tipo, o trabalho foi desenvolvido em dois níveis de pesquisa: exploratório e descritivo. Conforme Gil (2002), a primeira teve como finalidade conhecer melhor o problema, possibilitando a formulação de hipóteses.

A descritiva teve como objetivo a descrição das características de determinado fenômeno ou, então, o estabelecimento de relação entre variáveis.

O estudo exploratório foi amplo, porém superficial. Esse estudo visou extrair os subsídios iniciais para o desenvolvimento do trabalho.

No que se refere aos procedimentos técnicos, foram utilizadas a pesquisa bibliográfica e a pesquisa documental. A pesquisa bibliográfica se dá com “base em material já elaborado, constituído principalmente de livros e artigos científicos” (GIL, 2002). O mesmo autor descreve a pesquisa documental como muito similar à bibliográfica, estabelecendo como diferença essencial a natureza das fontes consultadas. A pesquisa documental se vale de materiais ainda não tratados de forma analítica ou dos chamados documentos de segunda mão que são aqueles que de alguma forma já foram analisados, tais como relatórios, no caso em questão, referentes ao Exército Brasileiro.

A análise dos dados se deu de forma qualitativa, na qual os mesmos foram reduzidos, categorizados, interpretados e expressos por meio de relatório coerente com o tema proposto (GIL, 2002).

A pesquisa bibliográfica foi realizada por meio de consultas às bibliotecas da Escola de Comando e Estado-Maior do Exército, da Escola de Artilharia de Costa e Antiaérea, do Centro de Instrução de Guerra Eletrônica, do Instituto Tecnológico da Aeronática e do Instituto Militar de Engenharia. Foram utilizados artigos científicos disponíveis em página eletrônicas da Internet.

Por fim, realizou-se pesquisa documental nos arquivos do Ministério da Defesa, do Exército Brasileiro e da Força Aérea Brasileira. Quanto à coleta documental foram consultados documentos oficiais do Ministério da Defesa, da FAB e do Exército Brasileiro.

3 ASPECTOS DOUTRINÁRIOS DA GUERRA CIBERNÉTICA

Tendo em vista a ampla gama de conceitos recentes relacionados ao tema da G Ciber, há a necessidade de abordá-los de forma a diferenciá-los, facilitando, assim, o correto entendimento dos aspectos doutrinários aplicados ao assunto.

3.1 CONCEITOS GERAIS

3.1.1 Cibernética

O termo refere-se ao uso de redes de computadores e de comunicações e sua interação com sistemas institucionais estratégicos públicos e privados. No sistema de Defesa Nacional, a cibernética abrange os recursos informatizados do Sistema Militar de Comando e Controle ($SISMC_2$), onde estão incluídos os sistemas de defesa aeroespacial (BRASIL, 2014d, p.18).

3.1.2 Espaço Cibernético ou Ciberespaço e Infraestrutura Cibernética

Entende-se como o ambiente composto por computadores de toda natureza, conectados em redes ou não, onde as informações digitais são processadas, transitam e são armazenadas. O conjunto de pessoas, processos e sistemas que constituem o espaço cibernético representam a infraestrutura cibernética (CARNEIRO, 2012, p.93).

3.1.2.1 Ativos de informação

São as pessoas, os equipamentos e os locais que se destinam ao armazenamento, a transmissão e processamento da informação, incluindo os meios de comunicações e de interconexão. Pode-se afirmar que fazem parte da infraestrutura cibernética (BRASIL, 2014e, p.18).

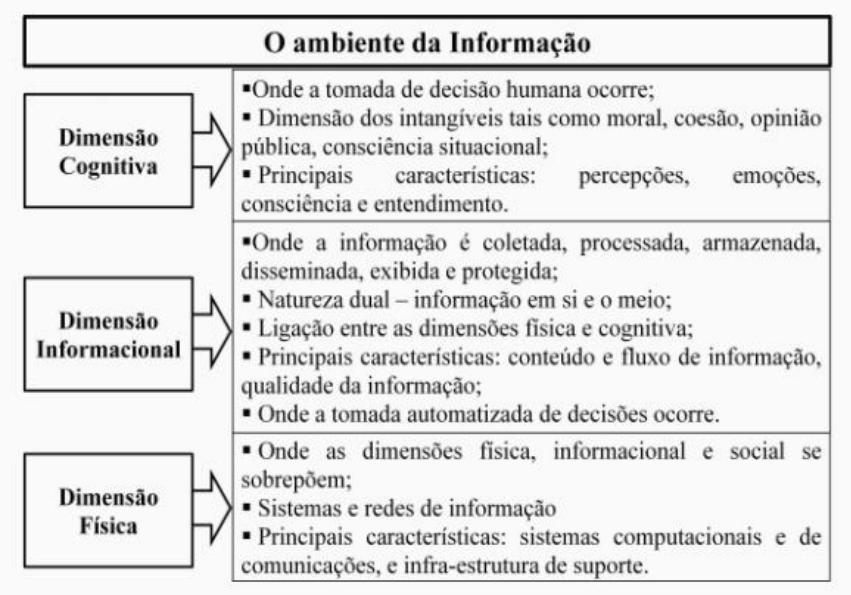
3.1.2.2 Redes no Ciberespaço

O ciberespaço consiste de muitas redes diferentes e seus nós de interconexão. Estando o ciberespaço altamente interconectado, facilita-se a transposição de fronteiras geográficas pelo uso da Internet. As Redes, entretanto, podem ser isoladas utilizando-se protocolos, firewalls, criptografia e separação física de outras redes. Podem ser agrupadas tipicamente em domínios, que podem ficar restritos a países, como no domínio brasileiro “.br”, ou atividades, como .”mil”, “.gov”, “.com” e “.org”. Estes domínios são específicos para uma organização ou missão e são organizados de acordo com a proximidade física ou função. Assim, pode-se restringir o acesso a uma rede de forma global ou remota. O acesso a redes fechadas e especializadas normalmente irá exigir maior proximidade física.

3.1.3 As Dimensões do Espaço Cibernético

Segundo Carneiro (2012, p. 81), o ciberespaço pode ser visualizado como três dimensões ou camadas (física, lógica e cognitiva) conforme se observa na Figura 1.

Figura 1 – Dimensões da Informação.


O ambiente da Informação
Dimensão Cognitiva
▪Onde a tomada de decisão humana ocorre;
▪ Dimensão dos intangíveis tais como moral, coesão, opinião pública, consciência situacional;
▪ Principais características: percepções, emoções, consciência e entendimento.
Dimensão Informacional
▪Onde a informação é coletada, processada, armazenada, disseminada, exibida e protegida;
▪ Natureza dual – informação em si e o meio;
▪ Ligação entre as dimensões física e cognitiva;
▪ Principais características: conteúdo e fluxo de informação, qualidade da informação;
▪ Onde a tomada automatizada de decisões ocorre.
Dimensão Física
▪ Onde as dimensões física, informacional e social se sobrepõem;
▪ Sistemas e redes de informação
▪ Principais características: sistemas computacionais e de comunicações, e infra-estrutura de suporte.

Fonte: Moresi (2011)

Nestas camadas estão os elementos que constituem os objetivos e as ameaças cibernéticas. A dimensão física abrange os equipamentos computacionais

(servidores, roteadores, terminais), as infraestruturas de rede (meios de radiodifusão, linhas telefônicas, cabeamentos ópticos e satélites) e suas posições geográficas. A camada lógica refere-se aos aspectos técnicos das conexões das redes de computadores, os programas e suas aplicações. A dimensão social ou cognitiva engloba o aspecto humano: o conhecimento, a identidade, as senhas, os endereços eletrônicos, os usuários, os administradores, os atuadores, os operadores, a criação e o desenvolvimento. Os ataques cibernéticos são direcionados para as dimensões física e informacional.

3.1.4 Domínios Operacionais

Os domínios operacionais se dividem em terrestre, marítimo, aéreo, espacial e cibernético, sendo interdependentes. A artilharia antiaérea normalmente se faz presente nas dimensões aérea, terrestre e marítima, sendo estes domínios regularmente permeados pelo cibernético.

3.1.5 Segurança Cibernética

É a propriedade do espaço cibernético que denota a habilidade de resistir a ameaças intencionais e não intencionais, responder e se recuperar.
Pode-se também afirmar que é a arte de assegurar a existência e a continuidade da sociedade da informação de uma nação, garantindo e protegendo, no Espaço cibernético, seus ativos de informação e suas infraestruturas críticas (CARNEIRO, 2012, p. 118).

3.1.6 Segurança da Informação e Comunicações

A Doutrina Militar de Defesa Cibernética (DMDC) define Segurança da Informação o conjunto de ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações (2014e, p. 19). Assim, pode-se afirmar que esse conceito está englobado na definição de defesa cibernética. Isso compreende a proteção contra a interrupção, negação, degradação ou destruição das informações residentes em computadores e redes de computadores.

Pode-se inferir que a Defesa Cibernética viabiliza o exercício do comando e controle, por meio da proteção dos ativos de informação, englobando as capacidades organizadas para mitigar e rapidamente se recuperar dos efeitos de um ataque cibernético. Na sequência serão apresentadas as características da Defesa Cibernética.

3.1.7 Defesa Cibernética

Existem variadas formas de definir defesa cibernética. Segundo Carneiro (2012) pode-se assim definir:

> " O conjunto de ações defensivas, exploratórias e ofensivas, no contexto de um planejamento nacional de nível estratégico, realizadas no espaço cibernético, com as finalidades de proteger os nossos sistemas de informação, obter dados para a produção de conhecimento de inteligência e de causar prejuízos aos sistemas de informação do oponente." (p. 18)

O foco da defesa cibernética está na salvaguarda de informações sensíveis e na eliminação da capacidade de atuadores adversos interferirem nas redes amigas. Assim sendo, os meios de transferência digital de dados e os sítios para postagem e disseminação de informações são prioritários para a proteção e a preservação da superioridade de informações (BRASIL, 2014d, p. 12-8).

3.1.7.1 Estudo das Características da Defesa Cibernética

Segundo o que se estabelece na DMDC, a D Ciber se baseia em dez características, entre as quais serão abordadas as de maior interesse para o estudo do da presente pesquisa.

A primeira característica é a insegurança latente, pois se considera que nenhum sistema computacional é totalmente seguro frente às ameaças cibernéticas ou de outra natureza, o que exigirá vigilância permanente dos gestores desses sistemas.

A segunda a ser abordada é o alcance global. A G Ciber pode ser conduzida simultaneamente em diferentes frentes de combate em qualquer lugar do globo. Assim sendo, dificilmente um sistema de comando e controle estará fora do alcance dos guerreiros cibernéticos.

A vulnerabilidade das fronteiras geográficas caracteriza a permeabilidade dos limites territoriais em relação aos ataques cibernéticos, uma vez que não se limitam a fronteiras geograficamente definidas. Essa característica reforça a do Alcance Global já mencionada.

No espaço cibernético as tecnologias e os atores se atualizam rapidamente e mudam os procedimentos constantemente, dificultando que limites legais mantenham eficácia contra as ações de G Ciber. A característica da mutabilidade condiciona para que não existam leis, normas ou comportamento imutáveis na defesa cibernética. Esse terreno sem leis exige postura pró-ativa por parte de gestores de TI.

No tocante ao Paradoxo Tecnológico, pode verificar que se trata de uma característica bastante evidente na D Ciber. Quanto maior é o estágio de desenvolvimento do oponente, maior é sua dependência da Tecnologia da Informação e, por conseguinte, mais propenso será às ameaças cibernéticas. Paradoxalmente, este mesmo oponente possuirá maior possibilidade de se defender dos ataques cibernéticos em virtude de seu alto grau de desenvolvimento tecnológico. Um exemplo clássico que se enquadra nesta característica são os sistemas de defesa aeroespacial, dos quais se exige uma estrutura de grande capacidade de defesa cibernética, caso da AAAe.

A defesa cibernética tem como característica ser Função Acessória. Suas ações são geralmente, empregadas para apoiar a condução de outros tipos de operação, ou seja, terá maior utilidade quando for conduzida em conjunto com outras ações como de inteligência, de guerra eletrônica ou de apoio à informação. As operações de informação são clássicos exemplos dessa integração da G Ciber com ações de outras naturezas.

3.1.8 **Guerra Cibernética**

Segundo definição da DMDC, G Ciber é o uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper, degradar ou destruir capacidades de comando e controle do adversário, no contexto de um planejamento militar de nível operacional ou tático ou de uma operação militar. Observa-se que são ações de combate.

A Guerra Cibernética compreende as ações que envolvem as ferramentas de Tecnologia da Informação e Comunicações (TIC) para desestabilizar os Sistemas de Tecnologia da Informação e Comunicações e Comando e Controle (STIC3) do oponente e defender os próprios STIC3. Abrange, essencialmente, as ações cibernéticas. A oportunidade para o emprego dessas ações ou a sua efetiva utilização será proporcional à dependência do oponente em relação às TIC (BRASIL, 2014e, p.19).

Segundo Fontenelle (2007, p. 2), a guerra cibernética deve ser empregada desde os tempos de paz, visando constituir um banco de dados para subsidiar ações ofensivas num emprego futuro. As ameaças atuam desde os tempos de paz, montando banco de dados para uso dentro das hipóteses de conflito ou para atuação no campo diplomático.

3.1.8.1 A Guerra Cibernética e as operações de informação

A G Ciber é um domínio global dentro da dimensão informacional do ambiente operacional. Consiste em uma rede interdependente de infraestruturas de TIC e de dados residentes, incluindo a Internet, redes de telecomunicações, sistemas de computadores e processadores embarcados e controladores (BRASIL, 2014b, p. 4-8). Afirma-se que as ações guerra cibernética fazem parte do conjunto das operações de informação, onde se incluem as operações psicológicas ou de apoio à informação, a guerra eletrônica e a comunicação social.

3.1.8.2 A Superioridade de Informação

Trata-se da vantagem decorrente da habilidade de coletar, processar, disseminar, explorar e proteger um fluxo contínuo de informações aos comandantes em todos os níveis, ao mesmo tempo em que se busca tirar proveito das informações do oponente, negando-lhe essas habilidades. É possuir mais e melhores informações do que o adversário sobre o ambiente operacional. É a condição que permite o controle da dimensão informacional (espectros eletromagnético, cibernético e outros) por determinado tempo e lugar (BRASIL, 2014b, Parte II). As Op Info contribuem para a obtenção da Superioridade de

Informações e integram capacidades como a Guerra Eletrônica, a Guerra Cibernética e a Inteligência (Intlg).

3.1.9 Sistema Militar de Defesa Cibernética (SMDC)

Ao SMDC cabe prover a proteção cibernética do Sistema Militar de Comando e Controle (SISMC2), para que este tenha capacidade de atuar em rede com segurança. Também cabe ao SMDC coordenar e integrar a proteção das infraestruturas críticas da Informação de interesse da Defesa Nacional.
O órgão central do SMDC é o Centro de Defesa Cibernética (CDCiber), que passa ao controle operacional do MD nas Operações Conjuntas e conta, permanentemente, com um Estado-Maior Conjunto para realizar o planejamento e o controle das ações planejadas, levando em conta as particularidades de cada Força Armada, de modo a obter uma atuação sinérgica (BRASIL, 2014e, p. 25).

3.1.10 As Ações Cibernéticas e os Níveis de Decisão

As ações cibernéticas se resumem no emprego de recursos do espaço cibernético com o objetivo de proteger os próprios ativos de informação; explorar e atacar redes do oponente, mantendo a capacidade de interferir no desenrolar das operações militares no Espaço de Batalha; bem como afetar as condições de normalidade em uma determinada área ou região, atingindo gravemente o funcionamento de estruturas estratégicas e serviços essenciais destinados à população. Classificam-se em ações de exploração, de ataque e de proteção (BRASIL, 2014b, p. 4-8).

3.1.10.1 Níveis de decisão das ações cibernéticas

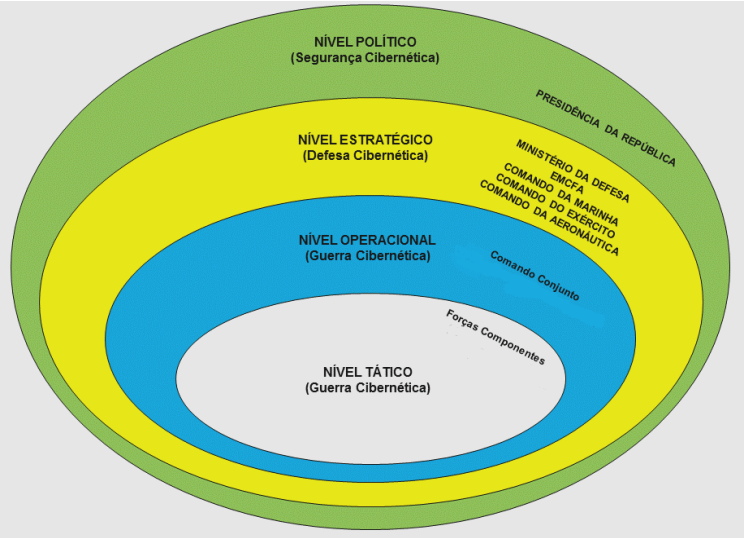
Os níveis de tratamento ou de decisão são: político, estratégico, operacional e tático. Estão ilustrados na Figura 2. De acordo com Carneiro (2012, p. 116) afirma-se que:

> “ No contexto do Ministério da Defesa, as ações no espaço cibernético, de acordo com o nível de tratamento, seguirão as seguintes denominações: - Nível político - Segurança da Informação e Comunicações (SIC) e Segurança Cibernética, coordenadas pelo GSI/PR e abrangendo a Administração Pública Federal direta e indireta, bem como as infraestruturas críticas da informação nacionais dos setores público e privado;- Nível estratégico: Defesa Cibernética, a cargo do Ministério da Defesa, interagindo com o GSI/PR e Administração Pública Federal.” (p ;116).

Assim, verifica-se que a Defesa Cibernética se aplica ao planejamento e execução das ações cibernéticas afetas ao nível estratégico de decisão. A denominação Guerra Cibernética está relacionada aos níveis de decisão operacional e tático conforme se observa na Figura 2. Sendo assim é restrita ao âmbito interno das Forças Armadas.

O nível operacional abrange as ações de Guerra Cibernética a cargo dos Comandos Operacionais e de seus Estados-Maiores, quando ativados.

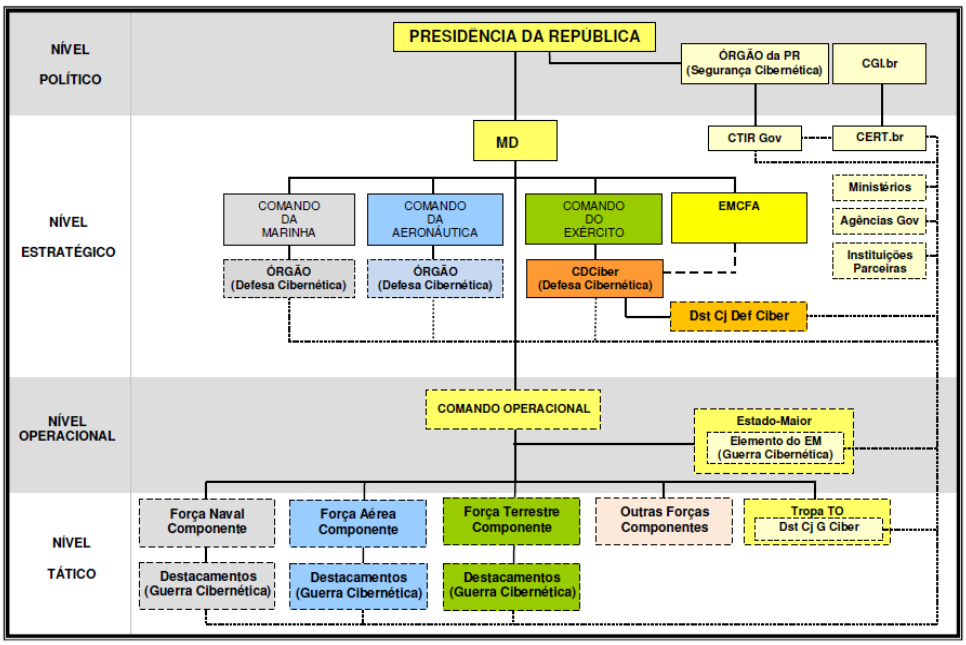
Figura 2 – Níveis de decisão



Fonte: Brasil (2014b)

No tocante ao nível tático, as ações de Guerra Cibernética ocorrerão dentro de um teatro de operações ou de uma área de operações, ficando a cargo das forças componentes o emprego de elementos de guerra cibernética com apoio prestado pelo Destacamento Conjunto de Guerra Cibernética, quando ativados. Isso pode ser verificado na Figura 3.

Figura 3: Dst Cj G Ciber no Teatro de Operações



Fonte: Brasil (2014e)

3.1.10.2 Os tipos de ações cibernéticas

Ao estudar o exposto na Doutrina de Operações Conjuntas (2011, p.56) verifica-se que as ações cibernéticas envolvem várias finalidades. As atividades de busca em sistemas de tecnologia da informação visando obter dados negados necessários à produção de conhecimento e ao levantamento das vulnerabilidades de tais sistemas caracterizam-se como exploração cibernética. As ações que tem por objetivo interromper, negar, degradar, corromper ou destruir informações armazenadas em dispositivos e redes computacionais e de comunicações de um oponente são consideradas ataque cibernético. As ações que neutralizam a exploração e os ataques cibernéticos de um oponente, protegendo dispositivos computacionais, redes de computadores e meios de comunicações próprios se enquadram na proteção cibernética. Sendo assim, observa-se uma semelhança entre as ações de guerra cibernéticas e as medidas de guerra eletrônica vigentes nas forças armadas: apoio à GE (análoga à exploração cibernética), ataque eletrônico e proteção eletrônica. Pode-se afirmar que a guerra cibernética e a guerra eletrônica são sistemas militares que se complementam, o que pode ser verificado no decorrer da presente pesquisa.

3.1.10.3 Estudo sobre os princípios de emprego da Defesa Cibernética

Conforme preconiza a DMDC (2014e, p 20), toda ação contra entidades cibernéticas deve produzir efeito que se traduza resultado vantajoso. Isso resume o Princípio do Efeito. Assim sendo, os alvos da guerra cibernética serão, normalmente, compensadores. Além disso, infere-se que para se obter algum tipo de efeito é necessário que tais alvos possuam alguma vulnerabilidade. Considerando esse princípio de emprego, é provável que se justifique uma ação cibernética contra um sistema de defesa antiaérea que não disponha de proteção cibernética devido à vantagem tática que poderá resultar. Logo, a proteção dos sistemas informatizados da AAAe é motivo de preocupação.

O Princípio da Dissimulação consiste em aplicar medidas para dificultar a rastreabilidade das ações cibernéticas ofensivas e exploratórias lançadas contra os sistemas de tecnologia da informação e de comunicações do oponente. Deve-se sempre mascarar a autoria e o local de origem dessas ações cibernéticas. Logo, infere-se que haverá dificuldade em identificar a ameaça e sua localização.

Para detectar ações cibernéticas contra os sistemas de informação e comunicações amigos é necessário existir estrutura de D Ciber e ligação, no mínimo um canal técnico. Isso se faz necessário para atender o Princípio da Rastreabilidade. Assim, para que um centro de comando e controle seja alertado e se proteja de um ataque cibernético deverá possuir recursos próprios de defesa ou capacidade de ligar-se com elementos de D Ciber que o apoiem. Essa condição deve ser atendida em um COAAe de Bda AAAe.

O Princípio da Adaptabilidade consiste na permanente adequação à realidade das constantes mudanças na dinâmica do Espaço Cibernético, o que exige proatividade, previsão e planejamento. Assim, são necessários profissionais e equipamentos capazes de operar diante de mudanças súbitas e imprevisíveis (BRASIL, 2014e, p. 20).

3.2 ASPECTOS DO NÍVEL OPERACIONAL DE DECISÃO

Conforme já observado, as competências do nível operacional cabem ao Comando Operacional e seu Estado-Maior Conjunto, os quais as exercem dentro do Teatro de Operações atribuído aos mesmos. Normalmente, o Comando do Teatro de

Operações receberá forças componentes e conjuntas adjudicadas ao seu controle e que realizarão as tarefas táticas a elas estabelecidas pelo referido comando. Em relação aos aspectos da G Ciber, uma das forças adjudicadas será o Destacamento Conjunto de Guerra Cibernética (Dst Cj G Ciber), cuja subordinação é direta ao Comando do TO, assim como as demais forças componentes adjudicadas. Logo, estará no mesmo nível das demais. Por ser uma força conjunta, normalmente irá atuar em proveito do TO, apoiando as demais forças sem estar sob o comando das mesmas (CARNEIRO, 2012, p. 127).

3.2.1 O Destacamento Conjunto de Guerra Cibernética

Segundo Carneiro (2012, p. 127) O Dst Cj G Ciber integra a tropa do TO vinculando-se à Célula de Op Info do Estado-Maior Conjunto. O destacamento pode ser constituído por militares do Exército, da Marinha e da Força Aérea. O efetivo mínimo que se propõem é de nove oficiais e praças especializados. Normalmente, o comando caberá a um oficial do Exército. Além dos militares, o destacamento poderá ser constituído por elementos de ligação interagências, como órgãos de segurança pública ou de defesa civil, e admitir especialistas civis que se façam necessários para operação e assessoria técnica. Sendo assim, o destacamento é uma força que pode reunir variados segmentos que atuam no espaço cibernético.

O detalhamento da estrutura e o efetivo do Dst Cj G Ciber será definido e proposto após estudo específico levando em conta as capacidades necessárias para cada Teatro ou Área de Operações. Caberá ao C D Ciber propor a estrutura e constituir o Dst Cj G Ciber. Caberá ao destacamento a difusão do nível de alerta cibernético estabelecido para o respectivo TO. Assim sendo, às demais forças componentes deverão possuir capacidades de adotar as providências defensivas cabíveis decorrentes do alerta. No nível tático, isso afetará os comandos envolvidos na defesa aeroespacial do teatro de operações.

3.2.2 O Estado-Maior Conjunto do TO e a Guerra Cibernética

A guerra cibernética em operações conjuntas deverá, em princípio, ser planejada e conduzida, no nível do Comando Operacional Conjunto, integrando a Célula de Operações de Informação. Sempre que possível, a Seção de Operações

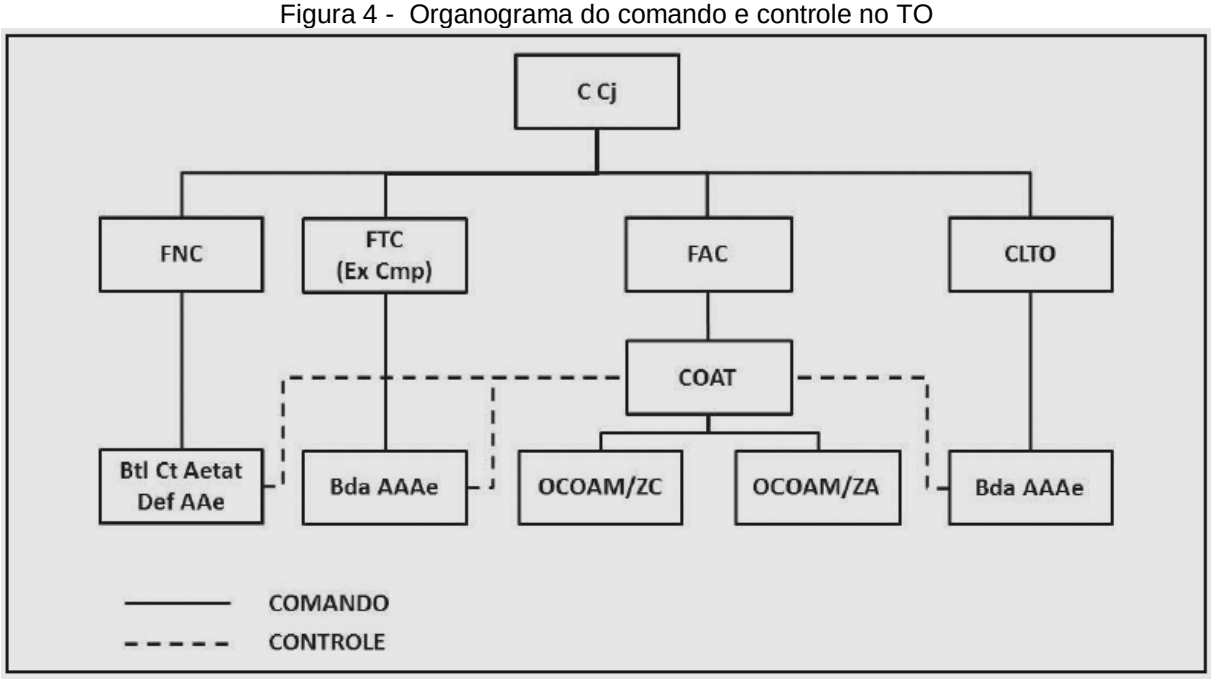
de Informação será formada por oficiais de Estado-Maior das três forças armadas especializados em G Ciber (BRASIL, 2014e, p. 29). Assim sendo, as missões do nível operacional atribuídas ao Dst Cj G Ciber serão integradas às demais tarefas de informação, o que inclui a guerra eletrônica.

3.3 ASPECTOS DO NÍVEL TÁTICO DE DECISÃO

As possíveis estruturas de Guerra Cibernética existentes na Força Terrestre Componente (FTC), na Força Aérea Componente (FAC) e no Comando Logístico do Teatro de Operações se enquadram no nível tático. Essas forças componentes poderão receber meios de AAAe adjudicados.

Logo, a Brigada de Artilharia Antiaérea opera neste nível de decisão da G Ciber. A Figura 4 complementa a Figura 3 na visualização das relações entre as forças componentes com a AAAe.

Figura 4 - Organograma do comando e controle no TO



Fonte: Escola de Artilharia de Costa e Antiaérea

Com base na atual doutrina de emprego da AAAe em operações conjuntas pode-se afirmar que, no Teatro de Operações, as Forças Componentes normalmente possuem elementos orgânicos de defesa antiaérea para a proteção de suas tropas, navios, instalações e, no caso da Zona de Combate, de pontos sensíveis em suas áreas de responsabilidade. O Comando Operacional poderá

também receber meios antiaéreos adicionais para emprego na Zona de Combate e meios para a defesa da Zona de Administração, ou seja, para todo o TO. Esses meios antiaéreos adicionais estarão sob comando de uma ou mais Forças Componentes, ficando dessa forma alocados no nível tático (BRASIL, 2011a, p. 56).

3.3.1 Atuação Cibernética Tática

Segundo Carneiro (2012, p. 124), a guerra cibernética tática é tipicamente empregada no contexto de uma operação militar, contribuindo para a obtenção de um objetivo tático. No entanto, as ações dessa atuação podem ocorrer tanto no nível operacional quanto no nível tático.

A fim de ilustrar, um exemplo de objetivo que resulte da atuação cibernética tática seria “Isolar, conquistar e manter uma determinada área, estabelecendo uma faixa de segurança, dentro de uma região em litígio. A inteligência de combate pode levantar que as forças oponentes utilizam determinadas redes computacionais e redes rádio para realizar o seu comando e controle e com isso alimentar a célula de Operações de Informação da FTC que, por sua vez, pode planejar um ataque cibernético de negação de serviço contra essas redes, sincronizado com medidas de ataque eletrônico contra as redes rádio levantadas, tudo isso, precedendo em poucos minutos uma manobra de desbordamento e cerco que seriam levadas a cabo por uma operação militar convencional. A perda de poder de combate decorrente da degradação dos sistemas de comando e controle do oponente pode contribuir para a obtenção do sucesso da operação. Isso pode ser feito de forma semelhante pela FAC por ocasião de ataque aéreo a uma área defendida por AAAe, neutralizando as redes dessa defesa oponente.

3.4 A G CIBER TÁTICA, OS PRINCÍPIOS DE GUERRA E OS FUNDAMENTOS DAS OPERAÇÕES.

Dentro dos princípios de guerra descritos na Doutrina Militar Terrestre (2014, p. 5-3) pode-se encontrar implicitamente a abordagem do emprego da G Ciber em nível tático nas suas definições. Assim, o princípio da ofensiva, impõe que uma força sempre mantenha a iniciativa das ações contra seu oponente para tirar vantagens das falhas adversárias existentes, retê-lo na defensiva, negar-lhe liberdade de ação

e abater o seu moral. Isso será mais rapidamente obtido com ataques contra os sistemas informatizados do inimigo, colocando em colapso os seus meios militares ao afetar os enlaces entre suas redes, principalmente se o oponente não possuir uma doutrina consolidada de Defesa Cibernética. Pode-se também afirmar:

> “ O emprego de uma ação ofensiva contra as redes do oponente para colocá-lo em uma situação desvantajosa e para concentrar um poder de combate esmagador no momento e local decisivo em um tempo ou modo em que ele esteja despreparado, atenderá os princípios da manobra, da massa e da surpresa, respectivamente, permitindo maior flexibilidade e maior poder relativo de combate ao atacante.” (PASINI, 2012, p. 72)

O princípio que destaca a importância do uso da G Ciber em um combate é o da economia de forças. Ao empregar um ataque cibernético nas redes computadorizadas dos sistemas de defesa do oponente gera-se um colapso nas suas infraestruturas críticas e, dessa forma, minimiza-se a dispersão de tropas em ações secundárias ou até dispensar o uso de um grande número de militares na ação principal. Já o princípio da surpresa descreve que será necessário proteger as redes computadorizadas e capacitar o efetivo em G Ciber para negar ao inimigo o uso da surpresa e impedir que ele interfira nos sistemas computadorizados.

Ao estudar os fundamentos das operações ofensivas preconizados no manual de fundamentos Operações (2014a, p.4-4), pode-se verificar que a importância do emprego maciço da G Ciber contra as redes dos meios de defesa do oponente terá como resultado a exploração de vulnerabilidades, a manutenção da iniciativa, a neutralização da reação do inimigo, a concentração do poder de combate e o aproveitamento do êxito, ao mesmo tempo em que pode garantir a segurança das tropas atacantes.

Nas operações defensivas, afirma-se que muito antes de uma tropa proteger o um determinado perímetro, é necessário existir a algum software de proteção nos seus sistemas informatizados contra *malwares* para poder garantir os fundamentos de segurança, flexibilidade e, principalmente, a defesa em profundidade (PASINI, 2012, p. 73).

3.5 CONSIDERAÇÕES

Entre os aspectos doutrinários estudados, observa-se que no nível tático de decisão, as ações de G Ciber possuem permeabilidade Cibernéticas em todos os domínios operacionais onde atuam as defesas antiaéreas, ficando a AAAe no alcance dessas ações, o que demanda medidas de proteção cibernética

Considerando que sistemas de AAAe são vanguarda em tecnologia e, por consequência, dependentes da Tecnologia da Informação. Logo, são mais visíveis às ameaças cibernéticas, o que exige maior desenvolvimento tecnológico para gerar novas capacidades de proteção cibernética. Isso obriga a AAAe a um ciclo contínuo de atualização de suas estruturas de Comando e Controle.

Verificou-se que a G Ciber prioriza suas ações com base no efeito resultante. Quanto mais vulnerável e compensador for o alvo, maior será o efeito e a prioridade de ataque. Assim sendo, sempre que os sistemas de C2 da AAAe não estiverem protegidos, os mesmo serão alvos prioritários da G Ciber.

Verificou-se que no TO os meios de AAAe podem ser adjudicados a todas as Forças Componentes, ficando a estas subordinados. Isso impõe a dispersão dos meios de AAAe em todo o teatro. O que vai exigir comunicações de longa distância. Isso faz com que a AAAe fique mais vulnerável às ações táticas de GE e de G Ciber, o que demanda recursos de proteção cibernética.

A Doutrina de Op Info revela que o planejamento da G Ciber é apoiado por meios de inteligência, podendo levantar dados sobre as redes do oponente. Assim se observa a importância do sigilo no que se refere aos sistemas de informação. Isso revela a necessidade de uma estrutura de segurança que atenda a todas as dimensões desses sistemas.

De acordo com a doutrina vigente uma Célula de Operações de Informação pode planejar um ataque cibernético sincronizado com medidas de ataque eletrônico, precedendo uma manobra de ofensiva convencional. Da mesma forma, essa ação preliminar pode ser feita em favor do sucesso de um ataque aéreo que necessite que uma defesa AAe seja neutralizada.

Diante do exposto, pode-se inferir que os aspectos doutrinários da Guerra Cibernética levantados apontam para a necessidade de estudar mudanças na atual estrutura de Comando e Controle da Bda AAAe do Exército Brasileiro.

4. A DOUTRINA MILITAR DE COMANDO E CONTROLE VIGENTE NO BRASIL

O entendimento dos aspectos relativos ao comando e controle militar é pressuposto básico para o estudo do funcionamento dos centros de operações dos elementos táticos das forças armadas, dos quais se destaca o Centro de Operações de Artilharia Antiaérea.

A Doutrina Militar de Comando e Controle (BRASIL, 2006) serve de subsídio para a o estudo desse assunto. O documento descreve a Guerra Centrada em Rede (GCR), a qual é um componente da Guerra Cibernética. Apresenta as características da GCR e descreve a importância da interoperabilidade entre as Forças Armadas. Estes e outros subsídios podem ser extraídos desta e de outras fontes pesquisa.

4.1 OS MODERNOS ASPECTOS DO COMANDO E CONTROLE

Além da abordagem da GCR se faz necessário o estudo dos demais conceitos afetos ao comando e controle na atualidade.

4.1.1 Comando e Controle (C^2)

Pode-se definir C^2 como a arte do funcionamento de uma cadeia de comando. Isso envolve a autoridade legitimamente investida da qual emanam as decisões que materializam o exercício do comando. As informações são os insumos para ao exercício do controle. Uma sistemática de processo decisório permite que haja formulação de ordens. Além disso, deve haver mecanismos para o fluxo de informações e que garantam o cumprimento pleno das ordens. Tudo isso é estruturado em pessoal, equipamentos, doutrina e tecnologias, o que permite o acompanhamento da evolução das operações por parte das autoridades (BRASIL, 2006, p.13). Um dos principais objetivos da atividade de C^2 consiste em permitir que uma autoridade tome decisões acertadas e no momento oportuno. Verifica-se que um sistema de comando e controle se resume em quatro elementos: tomador de decisão, informação, infraestrutura e processos.

A atividade de C^2 é desenvolvida por meio de centros de operações configurados para proporcionar as ligações na estrutura militar de comando, entre os

escalões superiores, de mesmo nível e subordinados. Cada centro de operações pode ser um Centro de Comando e Controle (CC²). Vários CC² subordinados a um mesmo comandante, interligados por enlaces de comunicações, formam a estrutura de C² desse comandante. Essa estrutura deve conter os recursos necessários para o fluxo de ordens e de informações para o exercício do comando (BRASIL, 2011a, p. 39).

4.1.1.1 Princípios de C²

As atividades de comando e controle deverão observar princípios básicos como unidade de comando, delegação de autoridade, simplicidade e segurança. Dependendo da situação operacional, os comandantes poderão atribuir maior importância a alguns princípios em detrimento de outros. O estudo será enfático em segurança.

De acordo com o princípio da segurança, ao se conceber um sistema de C², deve-se prever a segurança do mesmo, mediante criteriosa seleção de pessoal e uso de sistemas físicos e lógicos de acordo, com as normas de Segurança da Informação. Envolve treinamento de pessoal em procedimentos de segurança, emprego de sistemas criptológicos e por fim processos e técnicas seguras de troca de informações. Isso consiste em negar ou dificultar o acesso não autorizado às informações das forças amigas, restringindo a liberdade de ação do oponente em atacar o sistema de C². Para tanto, será indispensável dispor-se de informações oportunas e precisas sobre o sistema de C² do inimigo, incluindo suas capacidades de Guerra eletrônica e de Guerra Cibernética. As medidas de segurança devem ser continuamente revisadas, a fim de manter sua eficácia contra qualquer ameaça evolutiva. (BRASIL, 2006, p.18).

4.1.1.2 Estudo das Características de C²

A Interoperabilidade, a Confiabilidade e a Flexibilidade são particularidades e especificidades fundamentais que identificam um sistema de C². Os sistemas devem ter capacidade de intercambiarem serviços ou informações ou aceitá-los de

outros sistemas, unidades ou forças e empregar esses serviços ou informações sem o comprometimento de suas funcionalidades (BRASIL, 2006, p.18).

A interoperabilidade assegura que a informação possa fluir entre todos os comandantes e forças envolvidas em uma operação, principalmente em sistemas de C^2 que operam em ambientes conjuntos, combinados e multinacionais, integrados aos sistemas de outras instituições governamentais e organizações civis presentes em um TO. A interoperabilidade torna-se completa quando existir intercambio, compatibilidade e padronização entre os elementos constituintes de um macro sistema.

Pelo intercambio é possível que um componente seja substituído por outro similar, sem comprometimento de funcionalidades do sistema ao qual pertença. Havendo compatibilidade as partes de um conjunto podem adotar processos ou serviços que obedeçam a requisitos específicos sem causar falhas no sistema como um todo.

A padronização é a capacidade de desenvolver e implementar conceitos, doutrinas, procedimentos e propósitos comuns a diferentes sistemas voltado para alcançar um objetivo.

Um sistema de C^2 possuirá confiabilidade se possuir atributos de segurança, robustez e de continuidade de funcionamento. Esses atributos se resumem em validade das informações que transitam no sistema (BRASIL, 2006, p. 19). É nesses e outros atributos que a G Ciber atua de forma contrária.

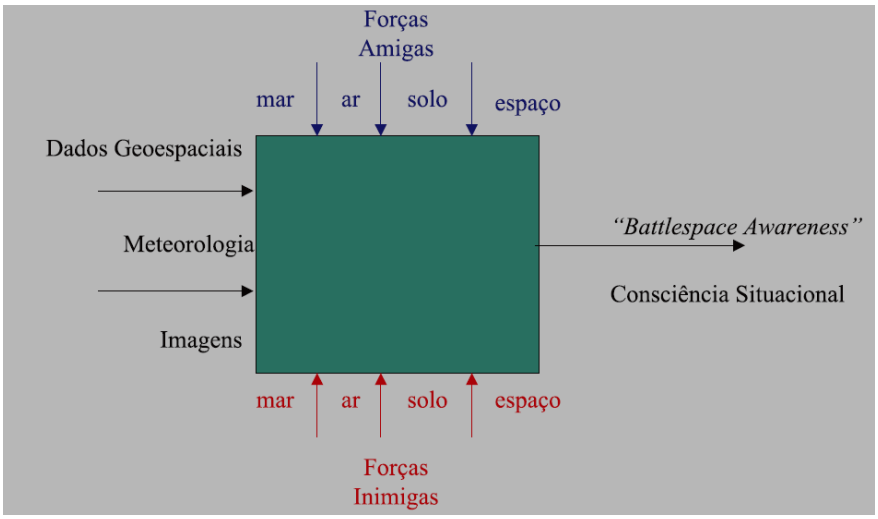
Um sistema de C^2 possui flexibilidade quando é capaz de modificar sua organização e suas funcionalidades de modo a atender a evolução da situação operacional. Deve ter capacidade para ser reconfigurado rapidamente e para responder rapidamente a uma mudança de ambiente, que poderá ocorrer, entre outros motivos, devido a ações de G Ciber. Para tanto, deverá ser capaz de agregar ou incorporar produtos e conceitos derivados de inovações tecnológicas, adequando se às reestruturações que se fizerem necessárias. Infere-se que as características mencionadas devem ser requisitos dos modernos centros de operações de AAAe.

4.1.1.3 Consciência Situacional

Um sistema de C² deve proporcionar a percepção precisa e atualizada do ambiente operacional no qual se atua e a ciência da importância de cada dado observado em relação à missão. Deve proporcionar perfeita sintonia entre a situação percebida e a situação real para que a autoridade tenha melhores condições para decidir. A formação da consciência situacional demanda significativo volume de informação sobre o ambiente de emprego, englobando conhecimento sobre as situações amiga e inimiga (BRASIL, 2006, p.23). Isso exige o funcionamento ininterrupto dos recursos de C²

Na era da informação, a vantagem está do lado daqueles que detêm a informação correta em tempo hábil, ou seja, quem possui a informação útil no mais curto prazo. A Consciência Situacional nada mais é que o domínio das informações que influenciam no teatro de operações. A Figura 5 apresenta algumas informações que compõem a consciência situacional no teatro de operações (SILVA, 2007, p.2).

Figura 5 - Informações da Consciência Situacional



Fonte: Silva (2007)

A limitação do tempo para as tomadas de decisão diante das ameaças aéreas exige que os sistemas de C² da AAAe forneçam informações em tempo real para que a formação da consciência situacional seja oportuna. Não será possível ter eficácia contra ameaças aéreas se o centro de operações sofrer interrupções em seu funcionamento.

4.1.1.4 A Importância da Função de Combate Comando e Controle

De acordo com a Doutrina Militar Terrestre, a essência das capacidades da F Ter reside na Liderança, nas Informações e nas Funções de Combate. As Funções de combate são Controle, Movimento e Manobra, Inteligência, Fogos, Logística e Proteção. Cabe ressaltar que todas as funções de combate são integradas por meio de atividades da Função de Combate Comando e Controle, o que caracteriza a sua importância em situações de guerra e de não guerra (BRASIL, 2014, 5-8).

No âmbito das operações conjuntas, a Célula de Comando e Controle da Força Terrestre Componente é composta pela Seção de Comando e Controle, pela Seção de Comunicação Social, pela Seção de Assuntos Civis, pela Seção de Operações de Informação, pelo Elemento de Guerra Eletrônica e por elementos de Operações Cibernéticas e de Geoinformação, integrando de forma sinérgica as capacidades afetas às operações de informação (BRASIL, 2014c. p. 4-2).

4.1.1.5 O Componente Informação

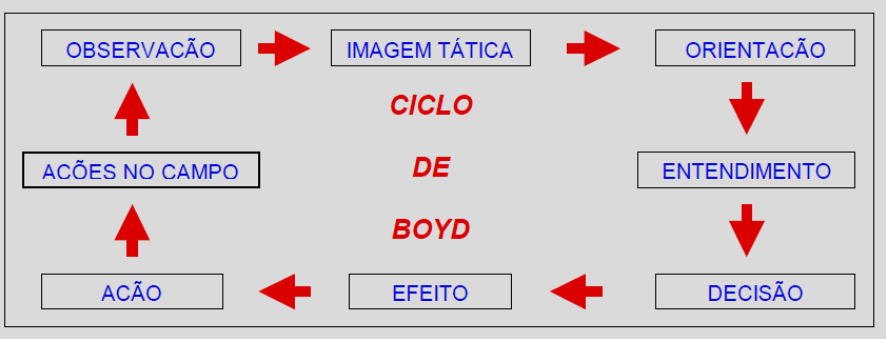
A Informação é insumo vital do comando e controle nas operações militares. Entende-se por Domínio da Informação como local onde a informação propriamente dita será criada, manipulada e compartilhada. Isso inclui as facilidades de troca de informações entre combatentes, o fluxo de informações entre as forças e a transmissão das ordens do comando. Esse domínio constitui-se num ambiente no qual as atividades Guerra Eletrônica e de Guerra Cibernética ocorrerão em conjunto somando-se às atividades de Inteligência e de Apoio à Informação. A integração de todas essas atividades com a Comunicação Social e os Assuntos Civis é a base para a condução das Operações de Informação (BRASIL, 2006, p.30).

Entende-se por Superioridade de Informação a capacidade de fornecer informações pertinentes aos usuários interessados, no momento oportuno e no formato adequado, negando ao adversário as oportunidades de atingi-la. Na disputa pela superioridade de informação, a manutenção do Domínio da Informação é requisito inegociável. A importância desse Domínio implica na necessidade de protegê-lo, pois disso advém a capacidade da própria força em gerar poder de combate e para fazer frente a um oponente (BRASIL, 2006, p.48).

4.1.1.6 O Ciclo da Tomada de Decisão

Conforme pode se verificar na Figura 6, a tomada de decisão se baseia em um ciclo que envolve observação, orientação, decisão e ação (OODA), conhecido como Ciclo de *Boyd*[1]. A velocidade da tomada de decisão dependerá da agilidade desse ciclo, cuja dinâmica reside em gerar rapidez às ações, fator decisivo para um comando e controle eficiente e vitorioso (BARROSO, 2004, p. 81).

Figura 6 - Ciclo de *Boyd*



Fonte: Barroso (2004)

As tomadas de decisão na AAAe são realizadas com tempo extremamente reduzido. Observa-se que as características do sistema de C² da AAAe, particularmente no que se refere ao acompanhamento da situação do espaço aéreo e ao engajamento de vetores aéreos hostis, se enquadram na dinâmica do ciclo OODA. Assim sendo, o sucesso da missão da AAAe é extremamente dependente de meios que gerem velocidade ao ciclo e que protejam seu funcionamento.

4.1.2 A Guerra Centrada em Redes (GCR)

Na Era da Informação surgiram novos conceitos, todos eles atuando sobre a informação ou nela centrados. Pode-se citar a Guerra de Informação e a Guerra Centrada em Redes. Baseando-se na atual doutrina militar de comando e controle pode-se afirmar:

[1] Conceito desenvolvido pelo Coronel John Boyd, estrategista da Força Aérea dos EUA. De acordo com Boyd, tomada de decisão ocorre em um ciclo recorrente de observar - orientar - decidir - agir.

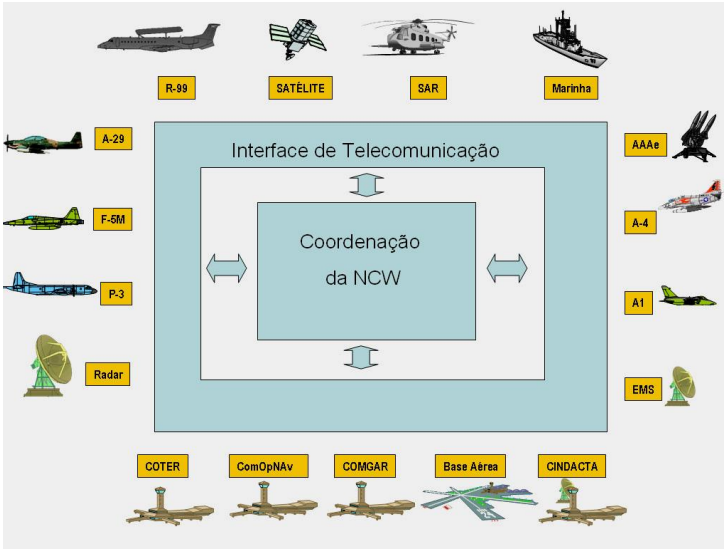
> “A Guerra Centrada em Redes é uma forma de atuar na guerra com a visão específica oriunda da era da informação. Caracteriza-se pelo estabelecimento de um ambiente de compartilhamento da consciência situacional, de modo a contribuir para a obtenção da superioridade de informação e da iniciativa, mesmo que os elementos da força estejam dispersos geograficamente.” (BRASIL, 2006, p. 47).

A GCR ou *Network Centric Warfare* (NCW) reconhece a informação como um insumo central nos conflitos atuais. Logo, é fundamental que a força disponha de Superioridade de Informação, pois isso cria vantagem frente ao oponente. Pode-se afirmar que esse conceito proporciona o aumento do poder de combate.

Na GCR trabalha-se o campo de batalha como uma rede integrada e dimensionada em sub-redes. Isso concorre para a melhora da mobilidade das peças de manobra, da coordenação entre elas e da utilização do conhecimento mútuo, diminuindo assim a duração do ciclo de C².

Afirma-se que o objetivo principal das operações centradas em rede é compartilhar o conhecimento de uma maneira mais eficiente e em tempo oportuno. Os principais receptores do conhecimento compartilhado são aqueles que participam das operações: o comandante e seu estado-maior (principais atores do sistema de C²) e os demais membros da força interessados. A Figura 7 apresenta de forma simples o fluxo e o compartilhamento das informações em uma rede de defesa aeroespacial.

Figura 7 – Compatilhamento das informações na GCR



Fonte: Silva (2007).

Sendo a GCR baseada em recursos de tecnologia da informação, pode-se afirmar que a uma das formas de um oponente reduzir o poder de combate de uma força que aplica este conceito é valer-se das ações de Guerra Cibernética.

A aplicação da Guerra Centrada em Rede exige a adoção de novas tecnologias e mudanças nas estruturas e nos comportamentos. A atual Doutrina Militar de Comando e Controle (2006, p. 47) estabelece que o conceito de GCR deverá ser acompanhado e aplicado nas oportunidades cabíveis de acordo com as possibilidades das Forças Armadas. Trata-se de um conceito impreterível na condução dos conflitos do século XXI. Assim sendo, deverá ser adotado no mais curto prazo possível nos comando de AAAe.

A GCR possui três domínios: físico, da informação e cognitivo (BRASIL, 2006, p.48). Para que o conceito de GCR seja aplicado se faz necessário que as forças estejam interconectadas nos três domínios. A simples interconexão física, requisito essencial, não é suficiente para aumentar o poder de combate. No entanto, atenção deve ser dada ao domínio físico devido ao fato de representar o ambiente onde ocorre o combate, onde ocorrerão as ações de ataque, defesa e manobra, seja naval, terrestre, aéreo e espacial. Neste domínio encontram-se as plataformas de combate e as redes que as interconectam.

Segundo o que estabelece a Doutrina Militar de Comando e Controle a GCR possui as seguintes características ou condicionantes:

> "1) Todos os elementos da força deverão estar interconectados de forma robusta e sem solução de continuidade.
> 2) A força terá a capacidade de compartilhar uma consciência situacional com seus elementos.
> 3) Os elementos de uma força serão capazes de sincronizar suas ações.
> 4) Capacidade da força em coletar, compartilhar, acessar e proteger a informação.
> 5) Desenvolver a posição geográfica dos seus elementos no ambiente operacional com maior facilidade e precisão." (BRASIL, 2006, p. 48)

4.1.3 O Sistema Militar de Comando e Controle (SISMC²) Brasileiro

O SISMC² é composto pelo conjunto de instalações, equipamentos, sistemas de informação, comunicações, doutrinas, procedimentos e pessoal essenciais para o comando e o controle destinado a atender as necessidades do preparo e do

emprego das Forças Armadas. Abrange os sistemas de comando e controle das Forças Armadas da responsabilidade do Estado-Maior Conjunto das Forças Armadas. Em situações extraordinárias, o SISMC² poderá ser interligado com o nível político, Presidência da República, o que exige segurança da informação. Esse sistema permite que o nível de decisão político atue no nível tático se necessário.

Os sistemas de comando e controle das Forças Armadas podem ser gerenciados por cada Força conforme seus interesses e peculiaridades desde que seja respeitadas as diretrizes gerais do SISMC² (BRASIL, 2011, p. 39). Isso permite que existam estruturas específicas para o comando e controle da AAAe.

Em relação aos recursos humanos, o SISMC² é composto por tomadores de decisão, assessores, pesquisadores e avaliadores e operadores. Aos operadores atuam em sistemas software, telecomunicações e enlace de dados. Dessa forma, devem ser proficientes na operação e na manutenção de STIC² e especializados de acordo com o equipamento, sistema ou sensor pelo qual são responsáveis.

Os recursos do SISMC² podem oferecer serviços como rede operacional, voz sobre IP (VoIP), correio eletrônico operacional, transferência de arquivos (FTP), rede privada virtual (VPN), acesso às redes internas de comunicações e de dados das FA, acesso seguro à Internet, videoconferência e sistemas de apoio à decisão. Todos esses serviços são baseados em TI. A Figura 8 apresenta uma videoconferência ocorrida durante uma operação a cargo do Ministério da Defesa.

Figura 8 - Videoconferência do Comando Conjunto

Fonte: Ministério da Defesa

Verifica-se que qualquer sistema de comando e controle que se integre ao SISMC² está suscetível à exploração e aos ataques cibernéticos.

De acordo com o Doutrina Militar de Comando e Controle, a infraestrutura do sistema abriga elementos necessários ao funcionamento dos CC² e dos processos de C². Esses elementos são:

> "a) Instalações – instalações físicas dos CC², centros de comunicações, quartéis generais e edificações que abriguem qualquer equipamento ou sistema do SISMC²;
> b) Equipamentos de telemática – computadores, switches, antenas, cabos de transmissão, receptores, transmissores, transcodificadores, etc;
> c) Sistemas de software de apoio à atividade de C² – sistemas de planejamento, sistemas de transmissão e acompanhamento de mensagens operacionais, sistemas de visualização do ambiente operacional, sistemas de análise e simulação e bases de dados operacionais;
> d) Sistemas e enlaces de comunicações – Sistema de Comunicações Militares por Satélite (SISCOMIS), Sistema Tático de Enlace de Dados (SISTED), redes de transmissão de dados e redes rádio; e
> e) Sistemas de sensoriamento – plataformas de sensoriamento e sistemas de processamento." (BRASIL, 2006, p. 30)

A Rede de Telefonia Pública Comutada (RTPC) poderá ser empregada como meio de enlace dos componentes do SISMC², desde que obedecidas as normas de Segurança da Informação do SISMC² em vigor. Isso exige adaptações por parte dos interessados nesta alternativa. É notório que, para um comando tático pode se integrar ao SISMC², é necessário atender a requisitos na parte de segurança da informação.

4.1.3.1 Órgãos do SISMC²

No quadro 2 estão listados os órgãos que fazem parte do SISMC²: O Centro de Comando e Controle do Comandante Supremo (CC²CS) é o órgão central do sistema, situado no MD. Os Centros de Comando e Controle dos Comandos de Teatro de Operações farão parte quando ativados.

Quadro 2 - Sistema Militar de Comando e Controle do Brasil

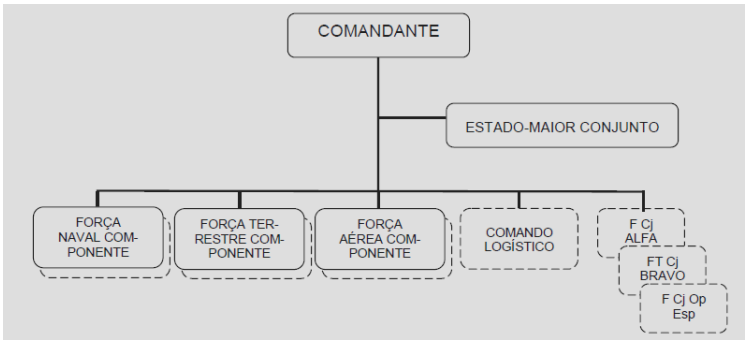
SISTEMA MILITAR DE COMANDO E CONTROLE DO BRASIL		
Ministério da Defesa	CC²CS	Centro de Comando e Controle do Comandante Supremo
	COCS	Centro de Operações do Comandante Supremo
Comando da Aeronáutica	CCCOA	Centro de Comando e Controle de Operações Aéreas
Comando do Exército	COTER	Comando de Operações Terrestres
Comando da Marinha	CCTOM	Comando e Controle do Teatro de Operações Marítimo

Fonte: o autor

4.2 ASPECTOS DO C² DO SISTEMA DE DEFESA AEROESPACIAL BRASILEIRO

O Sistema de Defesa Aeroespacial Brasileiro (SISDABRA) é responsável pela defesa aeroespacial do Território Nacional (TN). Da mesma forma, a Força Aérea Componente (FAC) poderá ter essa incumbência no TO, por delegação do Comandante do Comando Conjunto, devendo planejar e executar as ações de defesa aérea e antiaérea. A Figura 9 ilustra a composição de um Cmdo Operacional Conjunto.

Figura 9 - Comando Operacional Conjunto



Fonte: Brasil (2011)

4.2.1 Força Aérea Componente

A FAC é um conjunto temporário de unidades e organizações da Força Aérea que integram um Comando Operacional, o qual é organizado para a execução de uma missão específica, com objetivos e duração limitados, sendo desativado após o cumprimento da missão. A FAC pode ser composta por organizações destinadas à D Aepc do TO (BRASIL, 2005, p. 9). O Centro Conjunto de Operações Aéreas (CCOA) é órgão responsável, no âmbito da FAC, por planejar, coordenar e controlar as missões das unidades em controle operacional e, ainda, coordenar as operações de todos os meios aéreos operando em sua área de responsabilidade. A Figura 10 ilustra a célula de operações correntes de um CCOA desdobrado no TO.

4.2.2 Processo Básico da Defesa Aeroespacial

A D Aepc consiste basicamente na detecção de incursões de vetores aéreos e na atuação sobre esses vetores. Detectada uma incursão no espaço aéreo, busca-

se de imediato identificá-la e classificá-la. Tratando-se de uma incursão hostil, o sistema de defesa verifica qual a arma mais apropriada para responder à ameaça.

Poderá ser aeronaves de interceptação ou meios de defesa antiaérea. Normalmente, são alocados caças de interceptação em voo ou em alerta no solo para interceptar o mais cedo possível a incursão.

Figura 10 – Célula de operações correntes do CCOA

Fonte: ECEMAR

Caso os interceptadores encontrem dificuldades em neutralizar a incursão, existindo a possibilidade de ataques aéreos contra áreas ou pontos sensíveis, as defesas antiaéreas dos locais ameaçados passam à situação de alerta máximo para fazer frente à incursão, ficando para a artilharia antiaérea a responsabilidade de neutralizar as aeronaves inimigas. (BARROSO, 2004, p. 95). Observa-se que tal processo só é possível com o uso de meios eletrônicos de comando e controle.

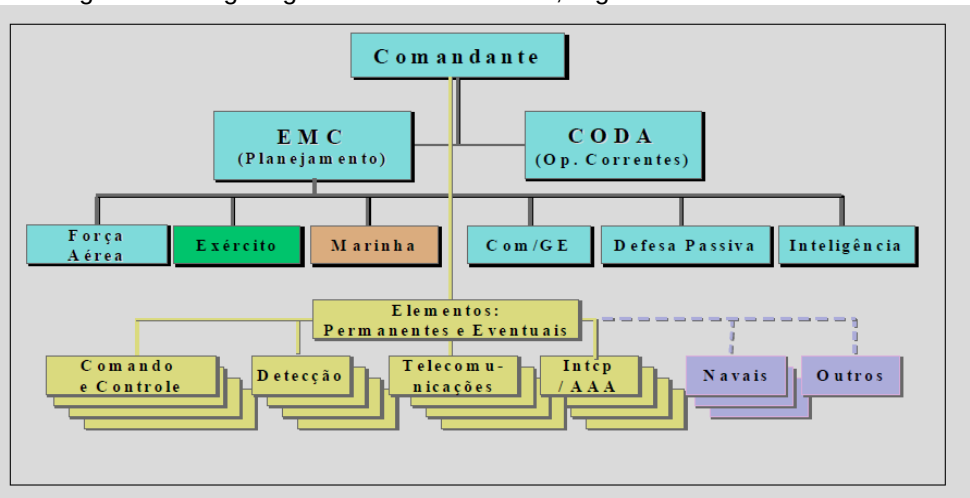
4.2.3 O Comando de Defesa Aeroespacial Brasileiro (COMDABRA)

O SISDABRA é composto basicamente por centros do comando e controle, por uma rede de radares de defesa, sistemas de telecomunicações e aeronaves de interceptação, de reconhecimento e de alarme antecipado / controle avançado (AEW&C). O SISDABRA também é composto por sistemas de defesa antiaérea. A D

Aepc compreende a D Aepc ativa (Ae e AAe) e a passiva. O órgão central do sistema é o COMDABRA, que é o Comando Operacional Conjunto responsável por conduzir a D Aepc do TN e também no TO, se a situação exigir. O COMDABRA está ativado de forma permanente desde o tempo de paz, tendo subordinação direta ao Comandante Supremo e ao Comando-Geral de Operações Aéreas (COMGAR). É componente da Estrutura Militar de Guerra (EMG), logo verifica-se que será integrado ao SISMC².

Ao COMDABRA cabe a defesa contra todas as formas de vetores aéreos, garantindo, na paz, soberania no Espaço Aéreo Brasileiro. Conduz a D Aepc na Zona do Interior (ZI) quando a estrutura militar de guerra for ativada. Na Figura 11 verifica-se os elementos que compõem sua estrutura. Dentro do COMDABRA, o Centro de Operações de Defesa Aeroespacial (CODA) é o órgão de C² que coordena e supervisiona todas as ações de D Aepc do TN (BRASIL, 2001, p. 3-4).

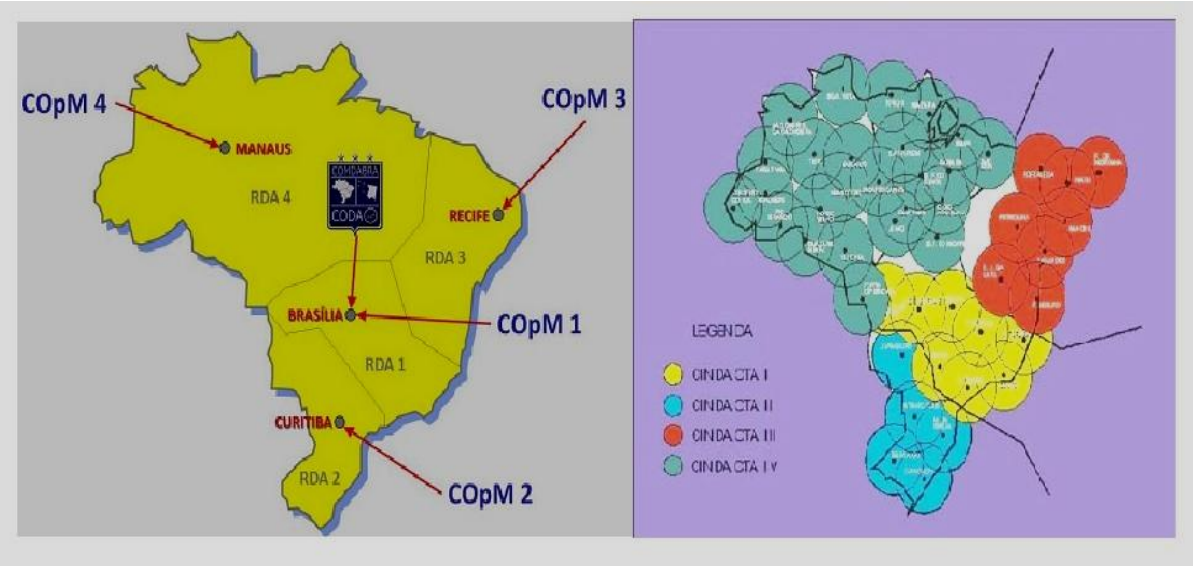
Figura 11 - Organograma do COMDABRA, órgão central do SISDABRA.



Fonte: Barroso (2004)

No Brasil, o TN é divido em quatro Regiões de Defesa Aeroespacial (RDA). Cada RDA possui um Centro Integrado de Defesa Aérea e Controle de Trafego Aéreo (CINDACTA), que por sua vez possui Centro de Operações Militares (COpM) que exerce as atividades de D Aepc da respectiva RDA através de um Órgão de Controle de Operações Aéreas Militares (OCOAM). Tal organização pode ser melhor entendida ao observar a Figura 12.

Figura 12 - Espaço Aéreo Brasileiro



Fonte: EsACosAAe, adaptado pelo Autor

Em caso de conflito, caso parcela do TO encontre-se dentro do território nacional, o COMDABRA pode transferir ao Comando da FAC a responsabilidade da defesa aeroespacial sobre porção do TN em conflito. Sendo o OCOAM (Figura 13) um centro de comando e controle que também é adotado no TO, este ficará subordinado à FAC. Neste caso o Departamento de Controle do Espaço Aéreo (DECEA) também pode transferir para a FAC a coordenação e o controle do tráfego aéreo civil, com o intuito de unificar as medidas de controle e coordenação do trafego aéreo no âmbito do TO.

Figura 13 - OCOAM

Fonte: Instituto de Controle do Espaço Aéreo

4.2.3.1 O Controle Sobre a Artilharia Antiaérea

Em todas as áreas de responsabilidade dos Comandos Operacionais ativados e mesmo na parcela do território nacional não incluída no TO haverá um órgão responsável pela defesa antiaérea. Na Zona de Interior o COMDABRA exerce o controle operacional de elementos de artilharia antiaérea do Exército distribuídos pelas RDA através dos COpM. A AAAe sob controle operacional é organizada em Brigadas de AAAe, integrando o SISDABRA. Doutrinariamente, cada RDA é defendida por uma Bda AAAe, cujo centro de controle estará normalmente justaposto ao COpM, o que facilita as ligações e a troca de informações (BRASIL, 2002, p. 2-3).

No espaço aéreo sobrejacente ao TO ou A Op esta responsabilidade pela D Aepc normalmente será delegada à Força Aérea Componente que eventualmente assumirá o controle operacional dos meios de AAAe da RDA englobada pelo TO. O TO normalmente possuirá duas Bda AAAe, uma na Zona de Combate (ZC) e outra na Zona de Administração (ZA). Normalmente os meios antiaéreos dispostos dentro da ZA permanecem sob controle operacional da FAC (BRASIL, 2011, p. 56). Verifica-se que a D Aepc é por natureza uma operação conjunta, particularmente no TO, o que exige a integração dos sistemas de C^2.

O controle no âmbito da AAAe é exercido por intermédio do centro de operações antiaéreas (COAAe) do maior escalão da AAAe da força, chamado de COAAe principal (P), o qual normalmente pertence à Bda AAAe responsável pela proteção de uma determinada região. Quanto ao escalão, o COAAe pode ser principal ou subordinado (S). Aquele que estiver ligado ao COpM será considerado principal. Os demais passam a ser subordinados.

O COAAe é por excelência o centro de C^2 da AAAe. Através dos COAAe se controlam e coordenam as operações da AAAe em seus diversos escalões. O Centro de Operações Antiaéreas Eletrônico de Brigada (COAAe Elt Bda) propicia, ao comando do escalão Bda AAAe, por meios eletrônicos, acompanhar, continuamente, a evolução da situação aérea e de controlar e coordenar as DA Ae desdobradas. Em seu estudo a respeito do comando e controle da AAAe, Barroso (2004) afirma:

> “ Percebe-se que há a necessidade, para um eficiente gerenciamento de C², da existência de pelo menos um COAAe P, capaz de fazer a interface com o OCOAM (COpM) da RDA. A realidade tecnológica atual aponta para o emprego do COAAe eletrônico, por ser mais capaz e eficaz nas atividades da DAepc, atendendo a agilidade requerida do Ciclo de *Boyd*.” (p. 148)

Verifica-se, assim, que toda a Artilharia Antiaérea presente no TO deverá estar com seus sistemas informatizados e integrados com os de D Aepc da FAC, o que melhora sua eficiência. No entanto, é possível que o sistema de C² da AAAe fique exposto aos ataques cibernéticos que o sistema de D Aepc da FAC venha a sofrer.

4.3 CONSIDERAÇÕES

Entre os atuais aspectos doutrinários de C² estudados, observa-se que a preservação do Domínio da Informação é uma exigência obrigatória, o que implica em soluções para protegê-lo. Ao se conceber um sistema de C², deve-se prever a segurança do mesmo, mediante criteriosa seleção de pessoal e equipamentos, sendo necessário treinamento de pessoal em procedimentos de segurança e uso de sistemas criptológicos. Um sistema de C² possuirá confiabilidade se possuir atributos de segurança, robustez e de continuidade de funcionamento.

É necessário que o sistema de C² seja flexível o suficiente para de adequar a uma mudança de ambiente decorrente de ações de G Ciber. Para tanto, o COAAe P deve incorporar inovações tecnológicas e ser reestruturado quando necessário.

A formação da consciência situacional na atualidade exige o funcionamento ininterrupto dos recursos de C², particularmente para permitir tomadas de decisão oportunas diante das ameaças aéreas. O centro de operações antiaéreas não será eficaz contra ameaças aéreas se sofrer interrupções em seu funcionamento em decorrência de ataques cibernéticos.

A velocidade da tomada de decisão depende da dinâmica do Ciclo de *Boyd* em gerar rapidez às ações. Logo o ciclo deve ficar isento de interferências hostis, em particular nas tomadas de decisão da AAAe onde o tempo de ciclo deve ser extremamente curto. Caso contrário, a missão da AAAe não será cumprida. Para obter uma significativa melhora na capacidade de observar, orientar-se, decidir e agir se faz necessário adotar o conceito de GCR.

Verificou-se que a GCR é estruturada em tecnologia da informação. Portanto, as ações de Guerra Cibernética podem reduzir consideravelmente o poder de combate de uma força que aplica este conceito. Dessa forma, a aplicação da Guerra Centrada em Rede exige a adoção de novas tecnologias e mudanças nas estruturas e nos comportamentos. Isso deverá ocorrer no mais curto prazo possível nos comandos de AAAe. Ao estudar a atual concepção do comando e controle da AAAe observa-se que se aproxima do modelo lógico da GCR. Infere-se, assim, que a adoção do conceito de GCR na AAAe acarreta em poucas mudanças.

O SISMC² pode oferecer diversos serviços seguros para o exercício do comando e controle. Observou-se que é possível que um COAAe P se apoie na estrutura do SISMC² desde que sejam respeitadas normas de segurança específicas. Conclui-se então que pode ser necessário inserir medidas de proteção na estrutura de comando e controle da AAAe. Além disso, para operar integrado ao SISMC² são necessários operadores capacitados em sistemas software, telecomunicações e enlace de dados, o que também pode acarretar em mudanças na atual dotação de pessoal do COAAe P.

Conclui-se que a Artilharia Antiaérea deverá estar com seus sistemas informatizados e integrados com os de D Aepc da FAC ou do COpM. Em qualquer dessas situações, o Centro de Operações Antiaéreas Eletrônico de Brigada (COAAe Elt Bda) é o que propicia condições de acompanhar a evolução da situação aérea e de controlar e coordenar as DA Ae, podendo fazer interface com o OCOAM. No entanto, é possível que o sistema de C² da AAAe fique exposto aos ataques cibernéticos que o sistema de D Aepc venha a sofrer.

De acordo com o apresentado, pode-se concluir que os aspectos atuais da doutrina de comando e controle C² estudados indicam a necessidade de possíveis alterações na atual estrutura de Comando e Controle da Bda AAAe do Exército Brasileiro.

5 RECURSOS DE COMANDO E CONTROLE EXISTENTES NO EXÉRCITO BRASILEIRO E NA FORÇA AÉRA BRASILEIRA

O estudo dos meios de C² existentes se faz necessário para o levantamento das vulnerabilidades dos mesmos frente às ações de G Ciber oponentes, particularmente no que se refere aos sistemas adotados na defesa aeroespacial. Com base nesse estudo buscar-se-á colher subsídios para embasar uma futura proposta de estrutura comando e controle que atenda à necessidade de proteção contra ameaças cibernéticas.

5.1 ESTUDO DOS MEIOS DE ENLACES DE COMUNICAÇÕES CORPORATIVOS

Os atuais sistemas de comunicações são convergentes com sistemas de informática. Esses sistemas estão estruturados em rede de computadores que dão suporte aos meios de transmissão de mensagens, possibilitando a o trâmite de dados em tempo útil. Em um *"backbone"*[1] podem se apoiar redes rádio, radioenlaces de micro-ondas e circuitos de fibra ótica. Isso permite integrar a rede de dados das diversas funções de combate, dentre as quais está incluída a de proteção.

No Brasil, os sistemas de comunicações das Forças Armadas não podem prescindir da característica básica de cobrir o TN, em face da necessidade precípua de C². Qualquer função de só poderá operar se dispuser ampla de capacidade de C², garantida por comunicações eficientes em todo o território nacional. (BARROSO, 2004, p. 77). Atendendo tal condicionante, entre os sistemas com possibilidade cobrir todo TN merece destaque o Sistema de Comunicações Militares por Satélite.

5.1.1 O Sistema de Comunicações Militares por Satélite (SISCOMIS)

O SISCOMIS é o meio principal de enlaces de comunicações que compõem a base física do SISMC². Compreende enlaces de longa distância, estabelecidos por

[1] *Backbone* ("espinha dorsal") é o termo utilizado para identificar a rede principal pela qual os dados de todos os clientes da Internet ou de uma rede grande rede corporativa. É o núcleo de rede que liga várias redes secundárias e forma uma grande e única conexão, sendo possível acessar qualquer rede por meio dele.

satélites, fibra óptica e redes metropolitanas, cujas conexões são obtidas por fibra óptica ou radiocomunicação. O sistema é gerenciado pelo EMCFA e vem sendo adotado tanto na FAB como no Exército Brasileiro. A Figura 14 apresenta uma visão abrangente do SISCOMIS durante a Operação Amazônia em 2012, onde se pode observar um terminal alocado para a Bda AAAe entre os terminais de defesa aeroespacial a cargo da FAC.

Figura 14 – Visão geral dos enlaces do SISCOMIS na Operação Amazônia 2012

Fonte: Ministério da Defesa

A origem do SISCOMIS data de 1985. O Sistema foi concebido para funcionar ininterruptamente, desde o período de paz, de modo a não sofrer solução de continuidade ao escalar para uma situação de crise ou de conflito. Atende principalmente ao Comandante Supremo, ao EMCFA e ao Comando das Forças Armadas, contudo pode fornecer enlaces para as grandes unidades do Exército. Desde o ano 2000 o sistema cobre todo o TN, incluindo as regiões Norte e Centro-Oeste. Opera nas frequências das bandas X, C e Ku, sendo composto por estações terrenas localizadas em centros urbanos, que distribuem a informação para outras estações fixas regionais, com enlaces por rádio ou por fibra ótica. O sistema da

banda Ku é capaz de prover acesso à Intranet e à Internet, acesso a correio eletrônico e serviços corporativos das FA, telefonias VoIP e pública (local e DDD).

Em campanha, os sinais são distribuídos através de Estações Táticas Transportáveis (ETT), que conferem mobilidade ao SISCOMIS no Teatro de Operações. As ETT fazem parte do SISTAC do Exército. Na Figura 15 observa-se uma ETT em operação (BASTOS, 2012, p 26).

Figura 15 – Estação Tática Transportável

Fonte: Bastos (2012)

Os satélites utilizados pelo SISCOMIS pertencem a Brasilsat, um grupo de satélites brasileiros operados, atualmente, pela empresa privada Star One, prestadora de serviço da EMBRATEL. São satélites destinados a também atender outras demandas de comunicações no Brasil. Não são utilizados exclusivamente pelas Forças Armadas e não estão gerenciados pelo Ministério da Defesa. Portanto, o SISCOMIS é dependente de Sistema Nacional de Comunicações (SNT), o que pode ser considerado um ponto vulnerável deste sistema.

Além do SISCOMIS, outros recursos de C² podem dar suporte ao funcionamento do SISMC², sendo acessíveis à Força Terrestre. São terminais transportáveis de radiocomunicação com criptofonia digital [2], meios dos órgãos civis e governamentais, redes de dados e de telefonia públicas e privadas e a Internet. Tais recursos adicionais carecem de rigorosas normas de Segurança da Informação, ou seja, necessitam possuir proteção contra G Ciber.

[2] Técnica de converter um sinal de voz claro em sinal ininteligível.

5.1.2 As Redes de Voz e Dados do EB

Atualmente as redes internas de comunicações de dados e de voz das três Forças são interconectáveis. As mesmas devem ser exploradas no que for de interesse para a estrutura de C² a ser estabelecida. Na doutrina vigente na Força Terrestre verifica-se a importância das redes e sua proteção.

> "As redes proporcionam ao Cmdo da FTC a capacidade de transmitir informações e controlar as operações dos seus elementos de emprego. São fundamentais para a obtenção e a manutenção da superioridade de informações e da consciência situacional – fatores que conduzem ao sucesso das operações militares. A proteção dessas redes – tarefa incluída na Função de Combate Proteção – deve ser uma preocupação constante, uma vez que elas se constituem em alvos compensadores para as ações do oponente e tendem a ser progressivamente degradadas no decorrer das operações." (BRASIL, 2014d, p. 8-6).

No Exército cabe ao Centro Integrado de Telemática do Exército (CITEx) a missão de proporcionar as bases física e lógica das redes para o funcionamento dos sistemas de interesse do Sistema Estratégico de Comando e Controle do Exército (SC²Ex), sua integração ao Sistema de Comando e Controle da Força Terrestre (SC²FTer) e ao SISMC².

5.1.2.1 Rede Corporativa Privativa do Exército (EBNET)

A rede corporativa privativa do Exército (EBNet) é composta por equipamentos digitais, capaz de suportar múltiplos serviços: voz, dados e imagens. No caso da Amazônia, a EBNET possui conexão junto ao Sistema de Proteção da Amazônia, o que demonstra sua capacidade de se integrar às demais redes das Forças Armadas. A rede possui segmentos com ligações de nível nacional (Comando do Exército – Comandos Militares de Área), nível regional (C Mil A – Grande Unidade) e nível local (Grande Unidade – Organizações Militares).

Em termos técnicos, a EBNet pode ser definida como uma rede IP/MPLS (*Internet Protocol/ Multiprotocol Label Switiching*). O IP é o protocolo de comunicação utilizado na Internet e que se encontra em franca difusão nas redes corporativas. O MPLS é um protocolo que redefine a tecnologia de roteamento de pacotes, o que permite a integração entre redes heterogêneas. Em termos práticos,

a rede IP/MPLS estabelece o melhor caminho entre a origem e o destino para uma dada aplicação e o mantém estável.

O CITEx firmou contrato com a EMBRATEL para fornecer infraestrutura e serviços de comunicação de dados, voz e vídeo entre OM específicas do EB, selecionadas para serem Pontos de Presença (PP). A rede dos PP constitui o núcleo da EBNet. As demais OM também tem acesso a este núcleo. A ligação pode se dar através de enlace direto por meio de uma rede metropolitana (*Metropolitan Area Networks* - MAN) e via Internet (rede mundial) empregando a tecnologia de rede privada virtual (*Virtual Private Network* – VPN). As organizações militares que acessam a EBNet por enlace direto são os PP, sendo as OM que hospedam os equipamentos da EMBRATEL, como é o caso da 1ª Brigada de Artilharia Antiaérea e suas OM subordinandas.

Em último caso, o acesso à EBNet ocorrerá por meio da conexão VPN, que cria um túnel criptografado para acesso seguro à rede a partir de um ponto que possua as credenciais necessárias e esteja ligado à Internet. Essa alternativa por vezes se faz necessária, porém é mais ariscada diante das ações da G Ciber. Pode-se verificar que a EBNET é uma rede dependente do SNT, ou seja, não é controlada exclusivamente pelo EB, o que exige cuidados quando à segurança.

5.1.2.2 Rede Integrada de Telecomunicações do Exército (RITEx)

A RITEx é uma rede de telefonia composta por centrais privadas de comutação telefônica (CPCT) digitais pertencentes a organizações militares normalmente chefiadas por Oficiais-Generais, que são interligadas por meio de circuitos estabelecidos em caráter exclusivo e privado. A 1ª Bda AAAe e suas OM subordinadas fazem parte dessa rede. O sistema é provido de tecnologia Voz sobre IP (VoIP[3]) e suas facilidades. Isso é possível por meio da ligação de uma CPCT a um servidor Asterisk VoIP, fazendo com que as OM não atendidas pela telefonia convencional sejam inseridas na RITEx através da telefonia IP, ou seja, por meio de computadores e aparelhos telefônicos ligados a redes IP internas ligados à Internet.

[3] VoIP (*Voice over Internet Protocol*), telefonia IP, telefonia Internet, ou voz sobre banda larga é um serviço suportado pela rede de computadores que consiste em digitalizar a voz em pacotes de dados para que trafegue pela rede IP e converter em voz novamente em seu destino.

Essa alternativa exige treinamento e proteção contra ameaças cibernéticas, pois também é um serviço prestado por operadora do SNT.

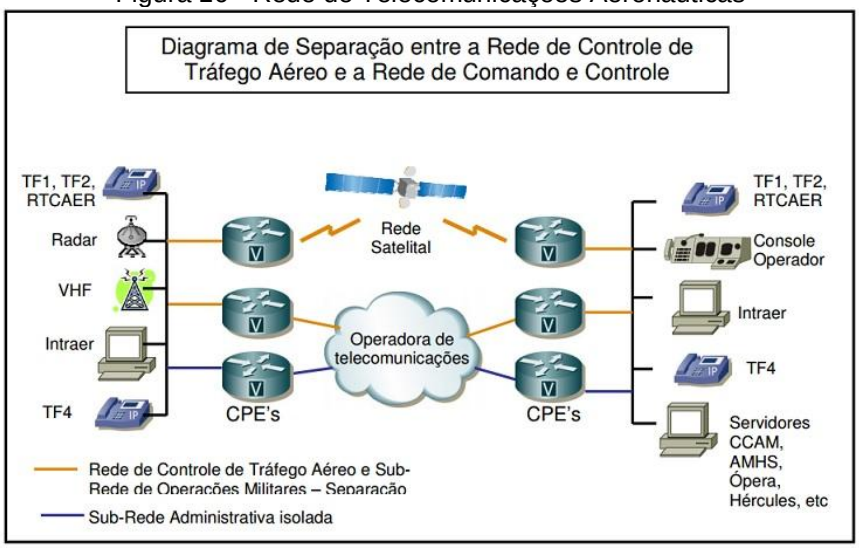
5.1.3 As Redes do SISCEAB e do SISDABRA

O Sistema de Controle do Espaço Aéreo Brasileiro (SISCEAB) e o SISDABRA possuem redes de comunicações específicas e compartilhadas dentro do Comando da Aeronáutica. A Rede de Telecomunicações Aeronáuticas ("*Aeronautical Telecommunication Network*" - ATN) estabelece comunicação entre os órgãos que compõem o SISCEAB, sendo destinada para tráfego exclusivo das aplicações que suportam os serviços de controle de tráfego aéreo e defesa aeroespacial.

Os meios de comunicação possuem alta disponibilidade e se baseiam em duas redes. O Sistema de Comunicações por Satélite emprega satélite comercial alugado junto à empresa TELESAT. A Rede de Telecomunicações Terrestre é contratada junto a operadoras de telecomunicações.

A Rede de Controle de Tráfego Aéreo (do SISCEAB) e a Sub-Rede de Operações Militares (do SISDABRA) possuem enlaces redundantes e são interligadas. Um dos enlaces pertence ao sistema de satélite e o outro é contratado junto à operadora de telecomunicações que utiliza meios terrestres de transmissão. (BRASIL, 2011, p. 7 a 14). As redes acima mencionadas são ilustradas no diagrama representado na Figura 16.

Figura 16 - Rede de Telecomunicações Aeronáuticas



Fonte: Brasil (2011)

A Intraer é a rede corporativa da FAB, semelhante à EBNET. Destina-se para comunicações e difusão de dados prioritariamente administrativos.

A Telesat é uma empresa com sede no Canadá que oferece serviços de comunicação via satélite para corporações e Estados. É proprietária dos satélites usados pelo SISDABRA. Além disso, o SISDABRA se apoia também se apoio em serviços prestados por operadoras de telecomunicações privadas em suas comunicações terrestres. Portanto, o Brasil não detém propriedade sobre a totalidade do sistema de comunicações usado no controle do espaço aéreo. o que caracteriza uma vulnerabilidade quanto ao sigilo dos dados.

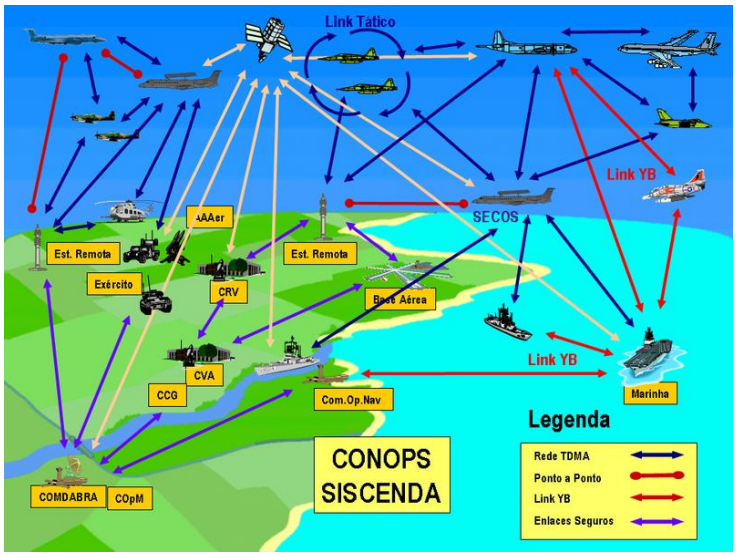
5.1.4 Sistema de Comunicações por Enlaces Digitais da Aeronáutica

Os primeiros sistemas de enlace de dados táticos surgiram no final da década de 50. Na Força Aérea Brasileira, o estudo para a implantação de um sistema de data link resultou com a implantação do Sistema de Comunicações por Enlaces Digitais da Aeronáutica (SISCENDA), sistema responsável pelo gerenciamento e coordenação da implantação do Link BR empregado no projeto do Sistema de Vigilância da Amazônia (SIVAM), que faz parte atual do atual CINDACTA IV. (ALVES, 2003 apud SILVA, 2007, p.2).

O uso desse sistema de *datalinks* consiste na conexão de estações terrenas com o E-99, aeronave de vigilância SIVAM. O sistema físico de computação (*hardware*) é de origem alemã e o *software do sistema* foi desenvolvido no Brasil, como o sistema de C^2 que opera no E-99. A AAAe pode ser incluída no SISCENDA, cuja concepção e os enlaces são ilustrados na Figura 17.

A aeronave E-99 é um elo vital do SISCENDA e um dos vetores mais importantes do sistema de defesa aeroespacial. Portanto, será um alvo compensador também para a G Ciber, que tentará alcançá-lo atacando o SISCENDA através de seus elos, a que pode ser um COAAe ligado ao sistema.

Figura 17 – Enlaces do SISCENDA



Fonte: Alves (2003)

5.2 MEIOS DE COMUNICAÇÕES DO SISTAC DO EB

O Sistema Tático de Comunicações do Exército (SISTAC), no nível Brigada, é composto principalmente de sistemas de enlaces empregados por tropas em operações. Destina-se a apoiar as necessidades de comando e controle, dos elementos subordinados e em apoio. Serão estudados os aspectos dos sistemas físico e de rádio para o emprego numa Bda AAAe.

5.2.1 O Sistema Físico

Os meios físicos de comunicações se caracterizam por propagar sinais confinados em cabos condutores, o que os torna menos vulneráveis às ações de Guerra Eletrônica. São exemplos: cabos telefônicos, cabos de fibra óptica e cabos coaxiais. São meios que se caracterizam por uma mobilidade restrita. Além disso, o alcance desses meios é dependente de fatores como características elétricas do circuito e a intensidade e natureza da energia gerada pelos equipamentos (BRASIL, C 11-1, 1997, p. 4-5). A fibra óptica possui excepcional taxa de transmissão de dados e é composta por material bom condutor de energia, sendo muito confiável quanto a perdas. No entanto, tem custo elevado, é frágil e apresenta forte atenuação em seu sinal a grandes distâncias, carecendo de aparelhos de amplificadores. A

abordagem da doutrina vigente no Exército a respeito do uso do meio físico no escalão Brigada é a seguinte:

> "O estabelecimento das comunicações por enlace físico nesse escalão apresenta grande sigilo frente à GE, mas seu emprego é limitado devido ao tempo disponível para o seu desdobramento, sendo utilizado em operações mais estáticas ou como complemento dos outros meios de comunicações em operações de movimento." (BRASIL, 1998, p. 4-11)

Diante disso, conclui-se que os sistemas físicos, embora mais seguros e confiáveis, são apropriados apenas para atender curtas distâncias (redes locais) em situações onde não há necessidade de constantes mudanças de posição dos centros de comando e controle. Essas condições por vezes são adequadas para um COAAe P, dependendo das circunstâncias da operação, porém os meios físicos normalmente não serão prioritários.

5.2.2 O Sistema Rádio

É o meio que permite a transmissão de mensagens por onda eletromagnética através do espaço. Seu funcionamento é pela utilização de frequências situadas em faixas do espectro eletromagnético, sendo as faixas HF, VHF, UHF e SHF as mais usadas pelo EB.

A faixa de HF é mais utilizada para comunicações militares a longas distâncias que não dependam tanto de largura de banda, pois possui baixíssima capacidade de transmissão de dados. Além disso, é uma faixa que o sinal transmitido pode sofrer reveses por fatores que provocam instabilidade e afetam a qualidade do enlace.

As faixas de VHF e UHF oferecem enlace com melhor qualidade e estabilidade, bem como bem como uma satisfatória taxa de transmissão de dados. Essas faixas são utilizadas em comunicações nos diversos escalões, desde grupos de combate até grandes comandos. No entanto, precisam de visada direta, o que limita seus alcances de transmissão e recepção, pois as ondas eletromagnéticas sofrem maior interferência do relevo, da vegetação e da umidade.

O rádio é o meio que oferece maior flexibilidade e rapidez de instalação. Contudo, exige maior grau de adestramento para que seu uso seja eficiente. A

manutenção é mais difícil e custosa que um sistema físico de comunicações, além de ser bastante vulnerável às ações de GE (BRASIL, 1997, p. 4-7 e 4-8).

Existe no SISTAC o sistema rádio por micro-ondas em visada direta (sistema multicanal). Este sistema admite ligações entre dois postos de comando. Normalmente é utilizado apenas nas ligações entre o PCP e o PCR de uma Bda; Também pode integrar o PCP considerado ao SISTAC do escalão superior (BRASIL, 1998, p. 4-7 e 4-8). A visada direta o torna razoavelmente seguro frente à GE. Outra vantagem é de permitir elevado tráfego de voz e dados a distâncias consideráveis.

Verificadas as características do sistema rádio confrontadas com as demandas atuais de um sistema de controle de uma Bda AAAe inserido no conceito da Guerra Centrada em Redes, conclui-se que os equipamentos que operam na faixa de HF não atendem às necessidades, pois os COAAe eletrônicos exigem rápido e elevado fluxo de dados, o que inclui imagens em tempo real. Devido aos aspectos negativos do rádio HF na cobertura de longas distâncias, o satélite (SISCOMIS) é a alternativa melhor, pois garante um enlace relativamente seguro, com a possibilidade de transmissão de dados de milhares de bytes como imagens aéreas e cartas topográficas, o que também reduz drasticamente a dependência do mensageiro para esses fins (BRASIL, 1997, p. 4-11).

A vantagem da transmissão a longas distâncias da faixa de HF pode ser aproveitada na troca de informações administrativas e como meio secundário, porém menos seguro, para o controle por voz.

5.2.2.1 O Rádio Definido por Software

Nos últimos anos, a pesquisa e o desenvolvimento de Rádios Definidos por Software (RDS) vem substituindo as implementações tradicionais em hardware para implementações mais flexíveis e programadas em software. O RDS é uma tecnologia emergente em que muitas as funções e recursos baseados em componentes físicos passam a ser substituídos por software. Dessa forma, o RDS permite aos usuários introduzir novas funcionalidades no decorrer do uso e do desenvolvimento do equipamento rádio.

Os RDS oferecem importantes vantagens para o desenvolvimento de soluções sem fio em sistemas de comunicações militares, o que inclui aplicações de

criptografia. Entre as características imaginadas, também se pode listar a interoperabilidade entre tropas de diferentes forças e nações, a portabilidade de formas de onda, e a possibilidade de atualização com os mais recentes avanços nas comunicações de rádio sem os requisitos de substituição de hardware (PAIVA JUNIOR, 2012, p.1).

O desenvolvimento de um rádio definido por software voltados para aplicações de defesa, pode empregar o padrão aberto de software SCA (*Software Communications Architecture*) e plataforma de hardware de baixo custo *Universal Software Radio Peripheral* (USRP), cujo exemplo está ilustrado na Figura 18.

Figura 18 - dispositivo URSP para RDS

Fonte: *National Instruments Corporation*

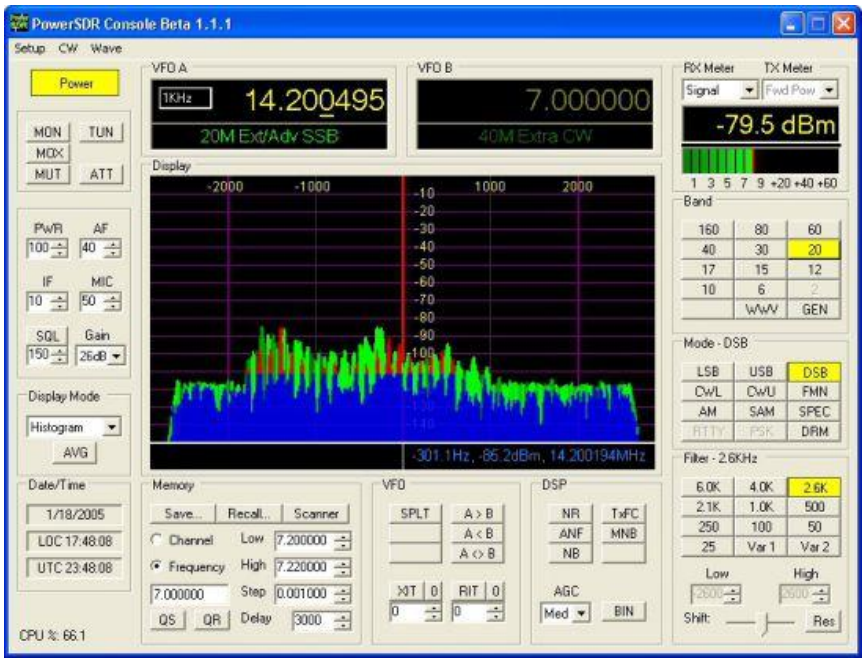
O padrão SCA foi originalmente proposto pelo programa *Joint Tactical Radio System* (JTRS), que é um programa para o desenvolvimento de rádios para operações militares patrocinado pelo Departamento de Defesa dos EUA. Assim, o padrão SCA/JTRS vem se tornando o padrão de fato para a construção de rádios militares. . O padrão especifica os mecanismos para criar, implantar, gerenciar e interconectar aplicações rádio, baseadas em componentes, em plataformas distribuídas. Isso aumenta consideravelmente a interoperabilidade nos sistemas rádio, bem como reduz o tempo de implantação e os custos do desenvolvimento de aplicações rádio. (PAIVA JUNIOR, 2012, p.2).

O desenvolvimento do RDS no âmbito das Forças Armadas existe desde 2012. O Projeto RDS é um empreendimento integra o Projeto Estratégico de Defesa Cibernética. O MD atribuiu a coordenação ao EB, que conduz o trabalho de

engenheiros das três Forças. Uma das características do rádio e a operação multibanda em HF, VHF e UHF. Observa-se que a nova tecnologia atende a diversos requisitos de proteção eletrônica e cibernética. O futuro RDS será compatível com o padrão SCA, baseado na versão 2.2.2. O projeto conta com a cooperação de engenheiros e técnicos das três Forças Armadas.

A parte física do RDS se limita ao equipamento USRP. É uma placa de baixo custo projetada para pesquisa e desenvolvimento de protótipos de aplicações em RDS. Isso permite aos desenvolvedores criar um rádio em software utilizando um computador pessoal por meio de uma porta USB. O USRP tem um projeto aberto e flexível, com a divulgação gratuita dos circuitos eletrônicos utilizados bem como dos softwares de integração de desenvolvimento rádio, como o GNURadio, Simulink e OSSIE. Os principais componentes da arquitetura do USRP são a antena, a placa-mãe e as placas-filhas. A antena de transmissão é responsável pela transmissão efetiva da informação através do canal rádio. De acordo com a necessidade do usuário, podem ser conectadas antenas em diferentes faixas de frequências (0 a 3 GHz), ou seja, o RDS admite múltiplas antenas para a transmissão e recepção de sinais. A Figura 19 apresenta ilustra um exemplo comum de RDS.

Figura 19: Console de RDS PowerSDR



Fonte: APRSBRASIL

5.3 ESTUDO DOS MEIOS DE COMUNICAÇÕES NA ARTILHIARIA ANTIAÉREA

Segundo Barroso (2004, p. 110) as comunicações são primordiais para o funcionamento do sistema de DA Ae. Caso não exista, os elos do sistema não são capazes de cumprir a missão de cooperar com a DAepc. A AAAe faz parte da solução do problema. Portanto, seus meios deverão ser capazes de atender de maneira eficiente as necessidades desta defesa.

5.3.1 As Características do Sistema de Comunicações da AAAe

A característica dominante na AAAe é a utilização quase exclusiva de meios de comunicações rádio. As redes rádio possuem grande número de postos descentralizados por todo a RDA ou TO, exigindo transmissões a longas distâncias. O sistema opera de forma contínua, operando muitas vezes com prescrições rádios livre ou mais permissivas que a tropa apoiada. Durante as incursões aéreas inimigas ocorrem picos de transmissão. Logo, verifica-se que o sistema fica constantemente exposto às ações de Guerra Eletrônica.

O meio rádio deve ser capaz de transmitir dados digitais em tempo real e interligar diferentes equipamentos de comunicações e transmissão de dados, ou seja, possuir interoperabilidade. O sistema deve ser robusto e resiliente para que continue operando sobre severas condições operacionais, particularmente sobre ataques eletrônicos, visando garantir a integridade das informações que trafegam na rede. Isso exige elevada resistência às medidas de ataque eletrônicas inimigas. (BRASIL, 2003, p. 4-1).

O sistema de comunicações exige ligações com outras Forças Armadas e com todos os escalões de AAAe. A moderna concepção do sistema de AAAe orienta para um sistema em rede, onde as unidades de emprego se conectam aos radares do sistema de controle e alerta, a fim de receber o alerta antecipado. Deve-se raciocinar com uma rede militar, cujas capacidades de seus postos sejam semelhantes aos dos computadores com acesso à Internet de banda larga. Diante disso, observa-se que o sistema exige também estruturas de proteção cibernética.

5.3.1.1 As Necessidades dos meios de comunicações da Bda AAAe

O Sistema de Comunicações de Brigada de Artilharia Antiaérea tem a finalidade de transmitir as informações, mensagens de dados e mensagens de voz para a coordenação e controle da DA Ae no nível Bda AAAe e para as ligações necessárias entre os elementos constituintes deste escalão.

De acordo com o que estabelece a doutrina vigente de emprego da AAAe os requisitos principais do sistema de comunicações para atender ao C² da Bda AAAe no território nacional são os seguintes:

> "(a) Comunicações por transmissão de dados entre o COpM da respectiva região de defesa aeroespacial e o centro de operações antiaéreas principal (COAAe P). A proximidade entre os dois C Ct facilitará a ligação, bastando apenas que exista um protocolo de comunicações único entre ambos para facilitar a interface dos sistemas de processamento de informações.
> (b) O COAAe P deverá manter ligações permanentes com os centros de operações antiaéreas subordinados (COAAe S), permitindo a transmissão dos dados das incursões repassadas a cada DAAe. Quando o ponto defendido for um órgão do SISDABRA poderá ser utilizada a rede de comunicações à voz privativa da FAe como dobramento de meios.
> (c) Na eventual existência de alerta aéreo antecipado fornecido diretamente por aeronaves de alarme aéreo antecipado (AEW), o COAAe P ou COAAe S deverão possuir condições de receber estes dados diretamente.
> (d) A ligação do C Cmdo da Bda AAAe com o das suas unidades subordinadas terá prioridade secundária em relação à ligação dos centros de controle." (BRASIL, 2003, p. 4-2)

No TO haverá comunicações externa com os COp da FAC, principalmente com o CCOA e OCOAM, utilizando um ou mais equipamentos para a transmissão de dados e voz para a coordenação dos meios AAAe empregados, particularmente da AAAe de média altura, e para as equipes de AAe (ELAAe) operando junto àqueles órgãos de C². Os meios de transmissão serão cabo, rádio e satélite.

Segundo Wurts (2003b, p.111, apud BARROSO, 2004, p. 185) uma forma de fazer a inserção segura na rede de comunicações da Força Aérea Brasileira, que emprega o *software* de criptografia SECOS, pode ser feita pela utilização de equipamentos rádio de pequeno porte. Afirma-se que o emprego de comunicações em HF, VHF e UHF são meios mais seguros que os que empregam satélites, pois são de custo mais baixo e independentes do controle por países estrangeiros e empresas privadas. O SECOS (*Secure ECCM Comunications System*) é o padrão de enlaces de dados do SIVAM, que faz repasse da síntese radar para os

interceptadores, dando uma visão comum da área de operações. O SECOS faz uso de técnica TDMA, salto de frequência e criptografia. Diante do exposto, é possível prover comunicações táticas seguras da AAAe com a FAB.

A ideia acima aponta para o estudo de uma solução baseada na família equipamentos rádio Harris Falcon III. Esta família tem a particularidade dos equipamentos serem RDS baseados em SCA, cujas capacidades da tecnologia já foram mencionadas. Além disso, possuem GPS integrados, o que permite mapear a posição de todos os rádios de uma rede. O modelo RF 7800M-MP opera em VHF e UHF, sendo capaz de transmitir dados por IP e de receber síntese radar oriunda dos sensores próprios ou dos demais escalões de AAAe vinculados, requisito exigido no funcionamento do COAAe P. Os modelo RF-7800W-OU440 pode transmitir a distâncias de até 90 Km. São equipamentos interoperáveis, o que permite comunicações com a FAC. Atendem ao conceito de GCR e que possui dispositivos de segurança para operar em rede (BUSCHER, 2013, p.65).

5.4 ESTUDO DOS SISTEMAS DE APOIO À ATIVIDADE DE C²

Ao estudar os recursos de comando e controle voltados para a missão da AAAe verifica-se a necessidade de enfatizar os sistemas informatizados empregados no SISDABRA, cujo uso nos é de grande importância COAAe P. O Sistema C² em Combate em desenvolvimento no Exército será abordado em segundo plano devido ao fato do sistema não ser voltado para defesa aeroespacial, embora seja de interesse do comando e controle de todas as funções de combate.

5.4.1. Sistemas Informatizados do SISDABRA

O processamento dos dados no SISDABRA exige rapidez e precisão, logo é feito por intermédio de sistemas informatizados, ou seja, por *softwares* que permitem a recepção e a difusão de mensagens, possibilitando um tempo para suficiente análise. Nos CINDACTA chegam todas as informações produzidas pelos radares desdobrados nas respectivas Regiões de Defesa Aeroespacial (RDA). Estas informações são utilizadas com duas finalidades distintas: a D Aepc e o controle do tráfego aéreo. As informações coletadas pelos radares são tratadas por um *software* específico que permite que os dados da síntese radar oriunda de uma eventual

ameaça aérea sejam visualizados nos consoles dos COpM. Isso permite a este centro o acompanhamento preciso do vetor hostil e o oportuno acionamento das U Ae D Ae e das U DA Ae. Isso também ocorre de forma semelhante no TO quando a defesa aeroespacial estiver a cargo da FAC.

5.4.1.1 O Sistema Defesa Aérea e Circulação Operacional Militar (DACOM)

O sistema DACOM é um sistema desenvolvido com características que permitem o rastreamento de aeronaves de alto desempenho e grande manobrabilidade. Permite visualizar 1024 pistas, pode se integrar a 32 radares e ligar-se com até 16 centros de controle, o que inclui os OCOAM aéreos e COAAe. Verifica-se que estas características atendem às necessidades de uma RDA ou a área de um TO. O X-4000 é software desenvolvido no Brasil que executa essas tarefas e que já esta sendo substituído por outra versão ainda mais completa. O sistema admite sete modos de trabalho para as posições operacionais do OCOAM entre as quais a destinada para a função de Oficial de Ligação Antiaérea (OLAAe).

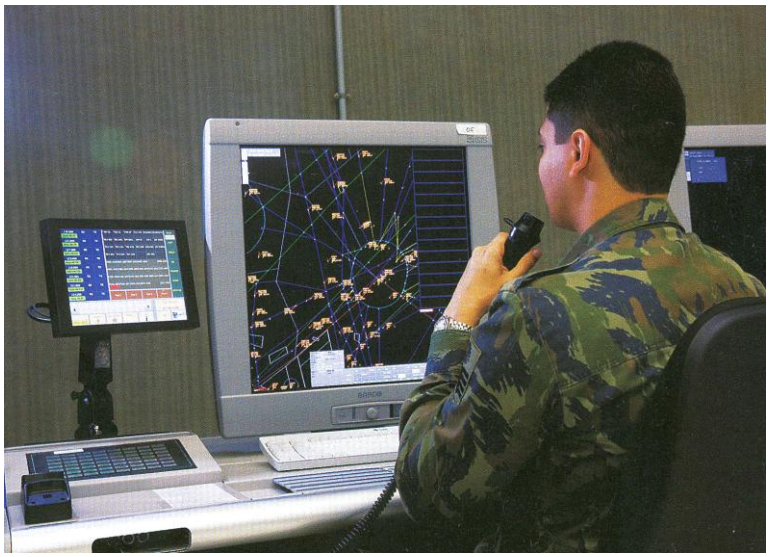
5.4.1.2 Estudando o Sagitário

O Sistema Avançado de Gerenciamento de Informações de Tráfego Aéreo e Relatório de Interesse Operacional, o SAGITÁRIO, é o substituto do software X-4000. O software, assim como o X-4000, é desenvolvido pela Atech, empresa brasileira de tecnologia. O novo software é capaz de processar dados de diversas fontes como radares e satélites e consolidá-los em uma única apresentação visual para o controlador de voo. A Figura 20 ilustra uma das formas de visualização apresentada na console ao controlador.

O Sagitário é inovador em relação ao programa X-4000. O software permite a sobreposição de imagens meteorológicas sobre a imagem do setor sob controle, o que permite acompanhar a evolução das condições na área a ser controlada.

Os planos de voo também podem ser editados graficamente sobre o mapa. Além disso, etiquetas inteligentes, por meio de cores diferentes de acordo com o nível de atenção para o cenário, indicam informações essenciais para o controle de tráfego aéreo (BRASIL, 2012).

Figura 20 – Console de operação do Sagitário



Fonte: COMDABRA

5.4.1.3 O Sistema de Transmissão da Situação Aérea Geral (SISTRASAG)

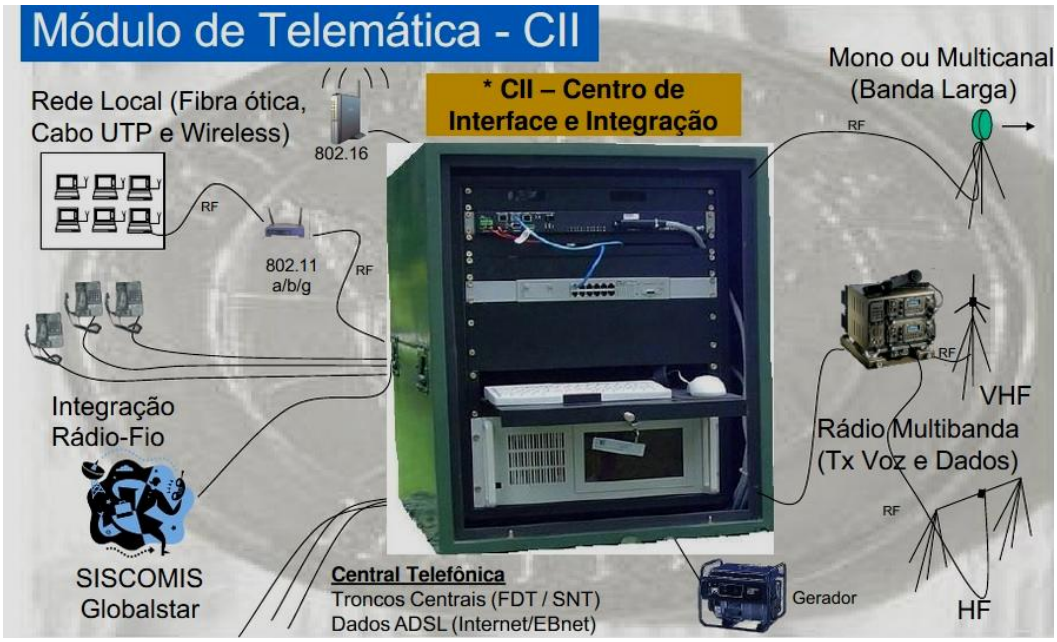
O SISTRASAG permite que informações de posição e estado de todas as aeronaves voando nos espaços aéreos sob jurisdição de uma Autoridade de Defesa Aeroespacial sejam transmitidos a qualquer COAAe qualificado para recebê-las. Os sinais são atualizados a cada 10 segundos. Pelo sistema é possível visualizar e acompanhar a situação aérea geral de todo o país, bem como a Situação Aérea Geral de Defesa Aérea (SAGDA). O SISTRASAG é uma redundância no fornecimento de dados de vigilância. Tem sido utilizado no COAAe P para monitorar atividades aéreas meio das imagens de radar fornecidas em tempo real pelo sistema.

5.4.2 O Projeto C² em Combate

O Projeto C² em Cmb é um diferencial tecnológico que está sendo disponibilizado pelo Departamento de Ciência e Tecnologia, por meio de seus órgãos subordinados (CIGE, CDS, DSG, CTEx). O sistema possibilita uma Bda e seus elementos subordinados exercer atividades de C² de forma automatizada e segura. O sistema permite a transmissão de voz, dados e imagens do campo de batalha em diversos meios de comunicações. Uma das finalidades do sistema é a integração do C² de todas as funções de combate, o que inclui a AAAe.

O programa está na 4ª versão. Tem capacidade de integrar rádios HF, VHF e UHF com transmissão voz e de dados por IP, redes Wirelles, satélite, telefonia celular de campanha, rede padrão Ethernet, telefonia fixa e modem ADSL. Isso confere ao sistema taxas de transmissão de 100 Mbps, acesso à EBNET e Internet, integração de sistemas de fonia e acesso a sistemas de telefonia fixa e móvel, tudo por intermédio de um módulo de telemática integrador. A Figura 21 representa a capacidade de integração do sistema.

Figura 21 - Integração dos meios de comunicações sistema C² Cmb

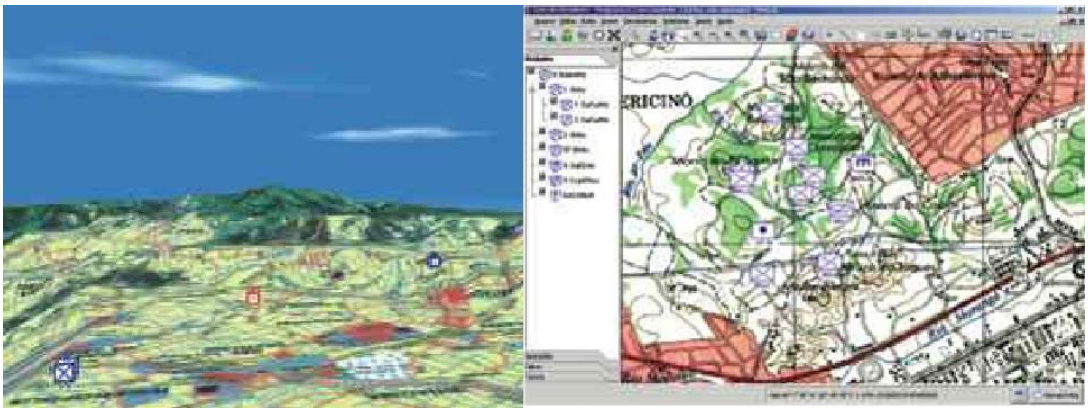


Fonte: Centro Tecnológico do Exército

Os recursos do sistema incluem também outras capacidades como a visualização de cartas digitais, tanto vetoriais quanto *"raster",* visualização gráfica do terreno e das informações em 3D (Figura 22), geração automática de mensagens e uso de criptografia forte e proprietária do EB. São capacidades que apenas as forças terrestres dos países desenvolvidos possuem.

Estes recursos permitem um aumento considerável na velocidade com que a informação fluirá através da estrutura de comando e controle, sem prejuízo da segurança e com incremento da capacidade de transmissão, atendendo a vários requisitos constantes do conceito da GCR.

Figura 22 - visualização gráfica do terreno



Fonte: Centro Tecnológico do Exército, modificada pelo autor.

5.5. CONSIDERAÇÕES

Diante do conjunto de informações apresentadas verifica-se a necessidade do COAAe P possuir interfaces de comunicações necessárias e suficientes para transmitir e receber dados e voz via SISCOMIS.

As distâncias dos enlaces podem superar 100 quilômetros, pois se considera a possibilidade da AAAe atuar na Amazônia e em outros pontos distantes do Brasil. Devido às atuais restrições do rádio HF para transmitir dados, o satélite da banda Ku (SISCOMIS) é uma alternativa, pois garante um enlace relativamente seguro com capacidade de transmissão de dados, sendo capaz de prover acesso à Intranet e à Internet. O sistema rádio de longa distância baseado em HF será meio secundário.

O COAAe P deverá ter capacidade de se integrar a variados sistemas baseados em Tecnologia da Informação, o que irá exigir pessoal especializado e capacidade de proteção contra ameaças cibernéticas. Deverá possuir conexão via EBNET, pois essa rede oferece a possibilidade integração com as demais redes das Forças Armadas, além de permitir comunicação com COAAe S remotos, o que exige especialistas capazes. Assim como o SISCOMIS, a EBNET e as Redes de Controle do Espaço Aéreo operam com serviços exclusivos contratados junto a operadoras civis de telecomunicações. Isso exige profissionais e equipamentos capazes de manter essas redes monitoradas contra ameaças cibernéticas.

Com a existência de alerta aéreo antecipado fornecido por aeronaves de alarme aéreo antecipado (AEW), o COAAe P deve possuir condições de receber estes dados diretamente. A aeronave E-99 é um elo vital do SISCENDA e um dos

vetores mais importantes do SISDABRA. Portanto, será um alvo compensador também para a G Ciber, que tentará alcançá-lo atacando o SISCENDA através de seus elos, que pode ser um COAAe ligado ao sistema.

Em curtas distâncias, o rádio continua a ser protagonista entre os sistemas que devem compor o COAAe P, particularmente na ligação com os COAAe S. O COAAe poderá usar o sistema rádio por micro-ondas em visada direta, que oferece maior proteção eletrônica. O sistema rádio deverá ser interoperável, sendo capaz de transmitir e receber dados e voz, e empregando plataformas e protocolos compatíveis com os sistemas de controle do espaço aéreo utilizados pela FAB.

Em relação à tecnologia a ser incorporada nos futuros materiais de AAAe, estudos apontam para a tendência de utilização de sistemas de satélite, do uso SNT, e de rádios, particularmente equipamentos definidos por software (RDS). O emprego de rádios definidos por software constitui a vanguarda no desenvolvimento de equipamentos rádio para aplicações militares, trazendo portabilidade de formas de onda e interoperabilidade entre diferentes Forças. Esse tipo de equipamento exige operadores dotados de novas capacidades. o RDS é uma solução que vai ao encontro dos requisitos de segurança exigidos para fazer frente a ameaças cibernéticas.

Os meios das telefonias privadas e da Internet são meios que poderão ser usados se necessário. Tais recursos adicionais carecem de rigorosas normas de Segurança da Informação, ou seja, necessitam possuir proteção contra G Ciber.

O sistema físico é mais seguros em relação a GE. A fibra óptica, embora possua excepcional taxa de transmissão de dados, tem custo elevado e é frágil. Assim sendo, só será alternativa nas situações onde não há movimento e que haja proximidade entre os COAAe.

De acordo com o apresentado, pode-se concluir que a complexidade e a variedade dos meios de C^2 disponíveis para o estabelecimento de enlaces no COAAe P revelam a necessidade de possíveis alterações na atual estrutura de Comando e Controle da Bda AAAe do Exército Brasileiro, o que vai exigir especialistas em telecomunicações, em redes de computadores e em segurança da Informação. Também se verifica a possibilidade do COAAe P ser dotado ou apoiado por equipamentos integradores, similares aos já conhecidos centros nodais de comunicação.

6. O EMPREGO DAS ARMAS CIBERNÉTICAS E AS MEDIDAS DE PROTEÇÃO

A ameaça cibernética coloca em risco a integridade de infraestruturas sensíveis, essenciais à operação e ao controle de diversos sistemas e órgãos relacionados à segurança nacional, o que exige a preocupação com as medidas de proteção. A proteção do espaço cibernético envolve inteligência, pesquisa científica, doutrina, capacitação, preparo, emprego operacional e gestão de pessoal. Compreende, também, a proteção de seus próprios ativos e a capacidade de atuação em rede.

Ao contrário da guerra convencional, a cibernética não se restringe às forças armadas de determinados Estados. Alguns países recrutam e investem em talentos humanos no meio civil.

6. 1 A GUERRA CIBERNÉTICA NA VISÃO DE OUTROS PAÍSES

Ao pesquisar a G Ciber, é possível afirmar que outras nações se encontram em estágios mais avançados que o Brasil no desenvolvimento da G Ciber.

> “China e Rússia vêm se destacando dentre alguns países que estão encarando como ação estratégica estatal a formação do que analistas estão identificando como “guerreiros cibernéticos”. Fontes especializadas asseguram que os chineses estão decisivamente engajados nas tecnologias de desenvolvimento de vírus e worms, bem como na abertura de brechas de segurança na Internet.” (PINHEIRO, 2008, p. 10).

Segundo Carneiro (2012, p. 91), nos últimos anos, os EUA, Rússia e China desenvolveram os seus próprios conceitos de Guerra da Informação, Operações de Informação e Superioridade da Informação. A visão norte-americana sobre esses conceitos é mais acessível, uma vez que esse país publica a maioria da sua doutrina ostensivamente em publicações conjuntas ou manuais de campanha.

6.1.1 A Guerra Cibernética na República Popular da China

O conceito chinês de G Ciber incorpora visões próprias sobre como fazer a guerra aos níveis estratégico, operacional e tático. A China é fortemente influenciada

pela ideologia marxista-leninista quanto esta modalidade de confronto. Muito de sua abordagem tem da ênfase no conhecimento, buscando vantagens assimétricas em relação ao adversário. Essa doutrina vem se desenvolvendo e gerando capacidades por de mais de 15 anos.

> “Em fevereiro de 1999, a editora oficial do Exército de Libertação do Povo divulgou um livro de autoria de dois coronéis – altos oficiais de política da Força Aérea da China − Qiao Liang e Wang Xiangsui. Traduzido para o inglês pela Central Intelligence Agency (CIA) em 228 páginas, o livro recebeu o título de ”Unrestricted Warfare” - Guerra Irrestrita.” (PINHEIRO, 2008, p.9).

Os chineses veem a G Ciber como uma transformação da guerra mecanizada da era industrial para uma guerra de decisões e controle, uma guerra do conhecimento e uma guerra do intelecto" (EUA, 2001).

Conforme afirma Carneiro, a doutrina chinesa considera que o combate às atividades do comando e controle é tão importante quanto à superioridade da informação, divergindo da doutrina dos EUA.

> “A China procura tirar proveito do fato de que, na área de Tecnologia da Informação, nenhuma nação pode se declarar dominante, o que não ocorre quando se trata de capacidade industrial ou equipamentos bélicos. Como resultado, a tecnologia da informação e a sua contraparte militar, a guerra da informação, são consideradas muito importantes para a China. A China visualiza os conflitos do futuro da mesma forma que os EUA, ou seja, conflitos limitados ao invés de uma guerra total. Para isto, o que mais deve ser enfatizado é o emprego combinado de medidas nos campos militar, político, econômico e diplomático. O objetivo não é esmagar o oponente, mas tornar o custo da guerra inaceitável. A doutrina chinesa considera que o “controle” (da atividade de comando e controle) é tão importante quanto a superioridade de informação. Da mesma forma que os russos, os chineses consideram que o primeiro leva ao segundo. A visão chinesa sobre operações centradas em redes é ligeiramente diferente da visão dos EUA, compondo unidades “mistas” de Guerra Eletrônica e Guerra Cibernética e chamando a sua teoria de Guerra Eletrônica e de Redes Integrada (INEW – integrated network-electronic warfare).” (CARNEIRO, 2012, p. 102).

Verifica-se assim que os elementos responsáveis pelo funcionamento de sistemas de comando e controle centrados em redes devem estar atentos aos métodos chineses de fazer a G Ciber.

As preocupações com as forças de redes da China cresceram após ataques sobre os sistemas de computador dos EUA e depois que a milícia chinesa realizou

exercícios de Guerra da Informação que tiveram a Índia, EUA, Taiwan e o Japão como países alvos. Esse treinamento teve como objetivo degradar e explorar a infraestrutura crítica desses países, incluindo o fornecimento de energia e as redes de telecomunicações, tudo de acordo com a abordagem chinesa de guerra assimétrica. Esses ataques partem de indivíduos, grupos e provavelmente de órgãos governamentais.

Afirma-se também que as Forças Armadas Chinesas invadiram os computadores das redes militares do Pentágono em junho de 2007, fazendo com que elas permanecessem fora do ar por mais de uma semana (MURPHY 2010, p. 24 apud PASINI 2012 p. 55). Segundo Fontenele (2007, p.1), esse ocorrido foi noticiado em publicação do *Financial Times* de Londres.

Diante do acima exposto, verifica-se também a necessidade de meios alternativos de fornecimento de energia elétrica aos sistemas de C². Isso inclui os meios de transmissão fixos que dependem da energia provida por empresas distribuidoras.

6.1.1.1 A Guerra do Povo

Assim como na Guerra da Informação, os chineses entendem que a G Ciber será realizada pelo Exército e pela sociedade como um todo, o que caracteriza a chamada “Guerra do Povo”. Este conceito tem encontrado expressão prática na transformação de parte das forças reservistas, de 1,5 milhão de soldados, em pequenos Regimentos de Guerra da Informação. A mobilização para a guerra pode se fazer pela Internet (CARNEIRO, 2012, p 103). Assim, a “Guerra do Povo”, pode ser realizada por centenas de milhões de pessoas usando modernos sistemas abertos de informação.

6.1.1.2 O Batalhão de Guerra da Informação

Em estudo realizado por Carneiro (2012, p. 36) verificou-se que a República Popular da China (RPC) criou um Batalhão de Guerra da Informação, situado na cidade de Guangzhou, oriundo de uma milícia local. O Batalhão foi organizado em torno das instalações de uma empresa de comunicações da região. A unidade integra em sua composição três companhias com missões distintas, porém

sinérgicas: uma Companhia de Comunicações, uma Companhia de Guerra Eletrônica e uma Companhia de Operações em Redes de Computadores. Essa composição demonstra a concepção chinesa de INEW, que se refere ao uso integrado da Guerra Eletrônica e das Operações em Redes de Computadores para interromper os sistemas de informação do inimigo, buscando a Superioridade da Informação.

Assim, fica evidente que as estruturas de proteção cibernética exigem também a presença de meios que permitam realizar as medidas de proteção eletrônica (MPE).

6.1.1.3 Métodos Chineses de Ataques Cibernéticos

No domínio cibernético, os chineses já adotam ao menos três métodos para atacar redes de computadores. O primeiro faz uso de correio eletrônico para infiltrar vírus. O segundo é o *phishing. e* por fim faz-se a introdução de "*trojans* inteligentes" e "*trojans* capturadores de dados". As ações de plantar *trojans* e vírus foram usadas para atacar computadores pessoais considerados críticos, que, por sua vez, passam a enviar arquivos ou causar danos na rede. Esses métodos não são inovadores e seus detalhes estão apresentados no decorrer do presente capítulo. São ferramentas simples e automatizadas usadas por de *hackers.* Como exemplo, um *trojan* capturador de dados pode extrair informações a partir de um *pen drive* automaticamente quando este for conectado a uma porta USB[1].

6.1.1.4 Ataques cibernéticos atribuídos aos chineses

Durante o ano de 2010, o Japão foi alvo de pesados ataques cibernéticos, por meio da ação de negação de serviço, contra sites do governo e de empresas de produtos de defesa japoneses. Segundo UMEZU (2011, apud PASINI, 2013, p 54), a *Mitsubishi Heavy Industries* (MHI), maior fornecedor de produtos de defesa, informou que detectou, em 11 de agosto de 2010, oito tipos de *malware em 45* servidores na sede central da empresa em Tóquio. O Estado teria verificado que 90% dos ataques foram oriundos da China.

[1] Universal Serial Bus: padrão de conexão permite a conexão de periféricos sem a necessidade de desligar o computador. Permite que vários periféricos sejam conectados a um mesmo canal.

Os chineses invadiram uma série de sites políticos, militares e diplomáticos dos EUA e também realizaram uma batalha de rede através da mobilização de milhares de usuários da rede para enviar e-mails e vírus. Isso fez com que os servidores ficassem sobrecarregados, paralisando um grande número de sites dos EUA. (CARNEIRO, 2012, p. 104).

Em 2012, A NASA foi vítima os de 5.408 ataques em seus computadores, que variaram desde uma simples contaminação por vírus até invasões organizadas vinda de outros países. Um ataque proveniente da China, principal concorrente dos EUA na atual corrida espacial, chegou a controlar os sistemas do Laboratório de Propulsão Nuclear (GOMES, 2012).

6.1.1.5 Comentários

A RPC deixa claro que a G Ciber esta em curso, levada em frente não só por soldados, mas também por *harckers,* cidadãos recrutados que podem controlar sistemas de informação. Suas ações são executadas de distintos pontos do globo e são capazes de destruir as informações contidas nos computadores de governos e de suas forças armadas.

6.1.2 A Guerra Cibernética nos Estados Unidos da América

A crise econômica de 2008 trouxe limitações à estratégia norte-americana. Houve severos cortes nos investimentos em todas as áreas, sobretudo na redução dos gastos em defesa. Isso fez com que o governo de Barack Obama adotasse outras formas de conduzir sua Política Externa e de manter sua hegemonia mundial. A G Ciber pode ser considerada um segmento de bélico de baixo custo comparando-se aos recursos aplicados nos setores aeroespacial e naval. A recente revelação sobre as ações de espionagem cibernética dos Estados Unidos deve ser entendida como parte da reestruturação da intervenção dos Estados Unidos no mundo que tem como diretriz a economia de suas ações.

6.1.2.1 Unidades de Guerra Cibernética do Exército dos EUA

Em julho de 2008, o Exército dos EUA divulgou a ativação de seu primeiro *Network Warfare Battalion* (NWB). Segundo Pinheiro (2008, p. 8) esta unidade não opera como um todo de forma independente, mas sim, por meio de destacamentos operacionais. Frações são alocadas ao comando de Grandes Comandos e Grandes Unidades. Essa forma foi aplicada no apoio às operações de combate nos Teatros do Iraque e do Afeganistão. O Batalhão participa também de Operações Cibernéticas (Cyber Operations) junto a elementos da Força Aérea (U.S. Air Force) e da Marinha (U.S. Navy) e em apoio a países aliados.

Além da Força Terrestre, todas as demais Forças Armadas norte-americanas estão engajadas no esforço conduzido pelo Departamento de Defesa para o desenvolvimento de sistemas ofensivos e defensivos de Guerra Cibernética (Cyber *Warfare*). As Forças Armadas dos EUA possuem, atualmente, dezenas de milhares de profissionais engajados em atividades dessa natureza. A tendência é que outras unidades especializadas valor Batalhão, e mesmo valor Brigada, venham sendo ativadas desde 2008 (PINHEIRO, 2008, p. 9).

Os EUA é uma referência na capacidade de desenvolver malwares militares, voltados para alvos específicos com capacidade para obter resultados pré-estabelecidos. Empregam-se ações de inteligência associadas à Engenharia de Software. Assim, desenvolvem a arma cibernética de forma semelhante à de um projeto de aeronave, com base em requisitos estabelecidos. Cabe ao Comando Cibernético do EUA (USCYBERCOM) levantar os alvos e coordenar o desenvolvimento de softwares para uso ofensivo contra os mesmos. (FINK e col., 2014).

6.1.2.2 Os investimentos em G Ciber nos EUA

Os EUA vêm acumulando os investimentos no setor cibernético de defesa a cada ano. Estima-se que o montante até então conhecido dos gastos do Pentágono em cibersegurança e cibertecnologia, tanto ofensiva como defensiva, podem superar 3,4 bilhões de dólares ao ano. Para ter ideia, o ciber-comando baseado em Fort Meade, criado em 2010, já teve previsão orçamentária anual de 154 milhões de dólares.

Dentro da política de desenvolver o setor, o Pentágono está acelerando o desenvolvimento de uma nova geração de ciber-armas mais nociva que o vírus Stuxnet (exemplo que será também estudado neste capítulo), capazes de destruir redes de comunicações militares inimigas mesmo que não estejam ligadas à Internet. Essas armas podem atingir alvos em sistemas militares *"off-line"* através de tecnologias novas que usam os sinais de rádio para acessar os códigos dos computadores em redes dificilmente acessíveis. Dessa forma, as formas já conhecidas de proteção serão pouco eficazes diante dessas inovações.

O governo norte-americano tem previsto 500 milhões de dólares de orçamento para financiar o desenvolvimento dessas armas e tecnologias de defesa nos próximos anos. O secretário-adjunto da Defesa e o vice-comandante das forças armadas americanas também alocaram milhões de dólares de orçamento para a Agência de Projetos de Pesquisas Avançadas de Defesa, o primeiro órgão de pesquisas do Departamento da Defesa. Esta mesma agência já lançou uma série de iniciativas de desenvolvimento da Internet, incluindo o *"fast-track program"*, ou seja, o programa de localização rápida.

Em relação ao atual ciber-arsenal afirma-se que o mesmo tem potencial para desativar componentes de um sistema de armas sem o destruir. Essas ferramentas são usadas associadas a outras táticas e armas. Até o momento a ciber-tecnologia pode apenas ativar ou permitir um ataque através do retardamento de reconhecimento desse mesmo ataque pela força inimiga (A VOZ DA AMÉRICA, 2015).

6.1.2.3 Doutrina de Proteção

Nos EUA as atividades de proteção cibernética se resumem nas Operações Contra-Ameaças Cibernéticas Defensivas (*Defensive CounterCyber Operations*). São as contramedidas defensivas realizadas para detectar, identificar, interceptar, destruir ou negar atividades maliciosas de penetração ou ataque através do ciberespaço.

Segundo Clarke (2010, apud CARNEIRO, 2012, p. 88), a estratégia defensiva norte-americana para conter ou mitigar os riscos trazidos pela cibernética se apoia em três medidas: defender o *backbone*, defender o sistema elétrico de geração e distribuição de energia e proteger as redes do Departamento de Defesa. Essas

medidas compõem a chamada Tríade Defensiva. Cabe ressaltar que o backbone interconecta redes de grande capacidade onde ocorre 90% do tráfego da Internet. A forma de realizar tal defesa se faz pelo monitoramento das entradas e saídas dos backbones. Ressalta-se assim a importância vital dos nós de rede e dos sistemas enérgicos.

6.1.3 A Guerra Cibernética na Rússia

Afirma-se que a Federação Russa desenvolve capacidades em Guerra da Informação e Operações de Informação. Diversas organizações russas são responsáveis por lidar com operações de redes de computadores, guerra eletrônica, operações psicológicas, campanhas de dissimulação e impacto de programação matemática. Este último é a atividade que se baseia na introdução de *malware* e funcionalidades como "*backdoors*"[2] e "bombas lógicas" (CARNEIRO, 2012, p. 96).

Segundo CARR (2011, p.1 61 apud CARNEIRO, 2012, p. 97), a Rússia tem sido um dos países mais ativos na implementação de ataques cibernéticos contra os seus adversários. Apesar de não ser possível provar que esses ataques ocorrem com a ordem ou anuência do Kremlin, os mesmos sempre favorecem o avanço das políticas russas e o governo nada faz para impedir esses ataques, beneficiando-se da situação. Isso ocorreu nos casos da Chechênia, Estônia, Lituânia e Geórgia.

A Rede de Negócios Russa é considerada a principal organização mundial no fornecimento de base logística para ciberataques e de outras atividades, sem motivações politicas, que encaixam no perfil de cibercrime. A atitude de benevolência das autoridades russas com essa organização indica que existe uma proximidade desta com os serviços de informações e segurança russos. Essa conduta encontra suporte na maneira de encarar este tipo de atividade na sociedade russa. Parte significativa da população não considera isso um problema para a nação e sim para os países ocidentais, alvos preferenciais dessas atividades.

Nos ataques cibernéticos direcionados contra a Estônia em 2007, um dos primeiros ataques cibernéticos publicamente conhecidos contra um país, utilizou-se

[2] Backdoor (porta dos fundos): Recurso utilizado por diversos malwares para garantir acesso remoto ao sistema ou à rede infectada, explorando falhas críticas existentes em programas instalados, softwares desatualizados e do firewall para abrir portas do roteador. Os backdoors podem ser explorados por sites maliciosos, através de vulnerabilidades existentes nos navegadores, para garantir acesso completo ou parcial ao sistema para instalação de outros malwares ou para o roubo de dados.

botnets e ataques distribuídos de negação de serviço em larga escala, lançados por grupos “civis nacionalistas”. De forma semelhante ocorreram os ataques contra a Geórgia em 2008. Na invasão da Geórgia houve um refinamento nas técnicas utilizadas, que ocorreram de forma sincronizada com a manobra dos meios militares que operavam de forma convencional, o que indica que houve coordenação entre os grupos de hackers e as Forças Armadas da Rússia. Foram utilizadas *botnets* pertencentes a um conhecido grupo de criminosos e fraudadores cibernéticos russos conhecidos como Russian Business Network. Este grupo atuava como um provedor de serviços internet e alugava servidores que podiam ser utilizados em crimes cibernéticos (CARNEIRO, 2012, p.98). Os dois incidentes mostram que pequenos grupos de pessoas qualificadas, fazendo uso de redes sociais para fazer recrutamento e prover um *malware a* ser utilizado por hackers, podem alcançar impactos significativos.

Pode-se verificar que o governo russo tem como doutrina fazer o uso da G Ciber como arma irregular aproveitando-se das capacidades de grupos de cibercriminosos e de nacionalistas simpatizantes das causas russas, o que apresenta algumas semelhanças em relação ao conceito chinês de “Guerra do Povo”.

6.2 AS AMEAÇAS CIBERNÉTICAS

Pode-se entender como ameaça cibernética os atores dotados de conhecimento e recursos e determinação para atuar contra sistemas informatizados de seu interesse e que exercem suas capacidades pelo emprego de ferramentas e técnicas baseadas em TI. Entre os podem estar agentes de Estados, grupos criminosos ou forças irregulares e entre as ferramentas estar os softwares mal-intencionados (*malwares*), técnicas e equipamentos.

6.2.1 Estudando o Malware

O termo "*malware*" é proveniente do inglês "*malicious software*" (programa malicioso). É destinado a infiltrar-se em um sistema de computador de forma ilícita, com o intuito de causar alguns danos, alterações ou roubo de informações. Ele pode aparecer na forma de código executável, scripts de conteúdo ativo, e outros

softwares. O termo "Malware" é utilizado para se referir a uma variedade de formas de softwares elaborados com finalidades ilícitas ou hostís. Os vírus, os Worms e os Trojans são os tipos mais comuns de malwares.

6.2.1.1 O Vírus e suas finalidades

Estrategistas do Exército Popular da China deram maior ênfase à guerra cibernética ao observarem a efetividade dos vírus de computador lançados pelos EUA contra o Iraque, na Guerra do Golfo, percebendo assim a potencialidade do seu emprego militar (BRANCO JÚNIOR, 2005, p. 58 apud PASINI, 2012 p. 55).

Vírus é um código malicioso que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos de um computador. O vírus depende da execução dos arquivos hospedeiros, textos ou imagens por exemplo, para que possa se tornar ativo e continuar o processo de infecção, ou seja, em geral depende que usuário execute o aplicativo infectado. Pode ser infiltrado de formas diversas, como através de meios de emails ou por arquivos em dispositivos de armazenamento.

O vírus tem por finalidade destruir ou corromper arquivos essenciais de um sistema, uma vez que sistemas de operacionais são compostos por um conjunto de arquivos. Os impactos mais comuns são a perda de arquivos importantes e a queda de desempenho dos sistemas, causando retardo no processamento e seu tempo de resposta. Esse retardo pode comprometer, por exemplo, a eficácia de um sistema de C^2. O efeito destrutivo pode ocorrer também sobre arquivos da memória interna de equipamentos, como memória ROM e EPROM, danificando o próprio hardware,

A quebra de determinados arquivos pode também criar brechas na segurança de um sistema deixando-o vulnerável a uma ação remota de um hacker.

6.2.1.2 O Worm e suas finalidades

Worm (verme) é um programa capaz de se propagar automaticamente através de redes de computadores, enviando cópias de si mesmo aos servidores e aos terminais das redes. Diferente do vírus, o *worm* não embute cópias de si mesmo em outros programas ou arquivos, não necessitando ser executado para se propagar. A

sua propagação se faz através de vulnerabilidades ou falhas na configuração de *softwares.*

O Worm é um arquivo independente e silencioso, podendo simplesmente ser instalado no sistema de computador sem ser percebido. Os *worms* podem instalar *backdoors, abrindo* brechas nos computadores para ataques via Internet. A partir disso, o *worm* pode tornar o computador infectado vulnerável a outros walwares e ataques. Quando a sua reprodução é elevada, danos podem ser provocados ao tráfego de rede, o que pode paralisar o fluxo de rede.

O worm pode infectar um terminal ou servidor várias vezes, causando negação de serviço pela sobrecarga das vias de comunicação do sistema, obrigando que algumas instruções fiquem em espera, o que inutiliza o computador depois de um tempo.

Computadores infectados (zumbis) podem ser usados de forma orquestrada por um hacker para enviar *emails* (*spams*) para diversos usuários e endereços de *sites* da Internet ou desencadear ataques DDoS (Ataque Distribuído de Negação de Serviço) propositais contra um determinado serviço da Web. Como exemplo, o worm Code Red explorava uma vulnerabilidade de estouro de *buffer*[3] dos servidores de web Microsoft IIS e se replicava. Quando acontecia o estouro do *buffer*, o servidor desligava. Os sites guardados nesses servidores que foram afetados pelo worm, exibiam a mensagem "*Hacked by Chinese*!"

Alguns vermes podem realizar atualizações indesejadas nos sistemas, o pode causar uma reinicialização inesperada máquina durante o processo de atualização, tornando os equipamentos inoperantes.

Verifica-se que, embora tenham a finalidade de explorar as vulnerabilidades nos sistemas que operam em rede, o maior impacto dos diversos efeitos dos worms é a paralisação dos sistemas.

6.2.1.3 O Worm Stuxnet e os malwares associados

Descoberto em 2010, o Stuxnet possui características de um worm clássico. Pode se autorreplicar e se espalhar de um computador para o outro. Além disso, conduz em si próprio um código oculto. O arquivo abre uma "porta nos fundos" nos

[3] Transbordamento de dados (*buffer overflow*): é uma anomalia onde um programa sobrescreve a memória adjacente. Esse é um caso especial de violação de segurança de memória.

equipamentos infectados, o que permite que esses computadores sejam controlados a partir de um local remoto pela Internet. (ALMADA, 2013, p.40)

Em seu funcionamento o Stuxnet busca por sistemas de controle industriais e então modifica seus códigos para permitir que os atacantes tomem o controle desses sistemas sem que os operadores percebam. Essa ameaça foi criada para permitir que hackers manipulem equipamentos físicos. É um worm inovador e sofisticado. É o primeiro malware capaz de causar dano no meio físico. De acordo com o veiculado pela empresa de sistemas Symantec, o projeto foi bem financiado, pois poucos grupos atualmente teriam a capacidade de criar uma ameaça desse nível, que tem como alvo específico sistemas de controle industriais (SYMANTEC, 2015).

De acordo com a observação acima exposta, seria impossível que um grupo de *hackers* conseguisse montar e implantar esse vírus sem um apoio de um Estado. Segundo Almada (2013, p. 20) é consensual, entre os especialistas, que o Stuxnet não poder ter sido produzido por um usuário doméstico até porque eram necessárias informações privilegiadas.

O Stuxnet deu o primeiro exemplo de destruição física por meio de um malware, foi criado para alterar o funcionamento de uma máquina forma que a mesma acabe danificada ou provoque danos. Segundo o estudo feito por Pasini (2012, p. 59) o Stuxnet danificou, entre o verão de 2009 e o outono de 2010, no mínimo, mil das nove mil centrífugas que estavam operando em instalações nucleares iranianas. Segundo o publicação da revista da OTAN, a disseminação do worm ocorreu em 2008 através de uma entrada USB de um computador portátil em uma base militar no Oriente Médio (THEILER, 2015).

Segundo Berman (2011, p. 45 apud PASINI, 2012, p. 39) o Stuxnet representa um tipo novo de guerra cibernética para o qual nenhum país está preparado. Sua disseminação pode ocorrer pela internet, pela intranet acessada por um *hacker* ou por pen-drive de um aliado.

Existem outros malwares que estão relacionados ao desenvolvimento do Stuxnet. São eles: Flame, Duqu e Gauss. Estima-se que o vírus Duqu também foi desenvolvido pela mesma equipe do Stuxnet, pois existem diversas semelhanças em ambos os códigos. O Duqu coletou as informações que foram necessárias para o desenvolvimento do Stuxnet.

O mesmo programa secreto que deu origem ao vírus "Stuxnet" também produziu a praga de espionagem "Flame", de acordo com uma reportagem do jornal norte-americano "*The Washington Post*", publicada em junho de 2012. O Flame teria sido criado para coletar dados de redes iranianas e preparar futuras ações. De acordo com estatísticas das empresas desenvolvedoras de antivírus, Irã e Israel são os países mais infectados. É considerado um dos malwares mais sofisticados da história para a finalidade de captura de informações (ROHR, 2012). Pesquisadores da Kaspersky Lab confirmaram que os autores dos vírus Flame e Stuxnet cooperaram em algum momento. Uma versão do Stuxnet de 2009 utiliza um código idêntico a um plugin do Flame, criando uma possível a ligação entre os dois malwares. O Flame seria resultado de uma colaboração entre Estados Unidos e Israel, segundo publicação do "*The Washington Post*".

O malware Gauss tem a mesma finalidade do Flame. É capaz de furtar credenciais, logins, informações de redes sociais, e-mails, dados da memória do PC e todo o conteúdo nele arquivado. A consultoria de segurança Kaspersky Lab afirma que o Gauss tem grandes semelhanças com o Stuxnet e com o Flame. Além de roubar dados de contas em serviços on-line, ele reúne informações obtidas na memória dos PCs infectados, incluindo o histórico de navegação na web, senhas e conteúdos armazenados em disco rígido. Ele infecta drives USB (pen drives) e outros dispositivos externos que sejam conectados a um computador hospedeiro. (O GLOBO, 2012).

6.2.1.4 Cavalo de Tróia (*Trojan*)

Os cavalos de Troia são malwares disfarçados de programas legítimos, sendo instalados diretamente no computador. Diferentemente dos vírus e worms, os Trojans não criam réplicas de si mesmo, motivo pelo qual não são considerados vírus. O programa se passa por um "presente" (por exemplo, cartões virtuais, álbum de fotos, protetor de tela, jogos, arquivos musicais, etc.) que, além de executar funções para as quais foi aparentemente projetado, também executa funções maliciosas de forma oculta ao usuário.

O Trojan representa o primeiro estágio de infecção de dispositivos digitais. Baixam e instalam ameaças mais robustas ao mesmo tempo que o usuário realiza atividades cotidianas. Podem ser transmitidos em mensagens de e-mail, downloads

de arquivos e em sites pornográficos, aproveitando as vulnerabilidades do navegador utilizado para acessar a praga.

Geralmente um cavalo de Troia é instalado com o auxílio de um ataque de engenharia social, com apelos para convencer a vítima a executar o arquivo do servidor, o que pode acontecer, dada a curiosidade do internauta, sendo atraído a ver fotos sensacionalistas mediante a instalação de um plugin, onde o cavalo de Troia pode estar hospedado.

Pode-se verificar que o emprego combinado dos malwares, associados a outras técnicas para empreender ataques cibernéticos, são condições básicas para o êxito dos empreendimentos dos hackers. Sem o malware as chances de sucesso ficam limitadas. Sendo assim, uma das primeiras medidas defensivas será o bloqueio e a neutralização dos malwares e suas formas de difusão, o que exige softwares antivírus eficientes e conhecimento em proteção cibernética.

6.2.1.5 Backdoors

São malwares normalmente usados para garantir a um atacante uma forma de retornar a um computador comprometido, sem precisar recorrer aos métodos utilizados na realização das primeiras invasões. A intenção do atacante é poder retornar ao computador comprometido sem ser notado. Portanto, o invasor instala um programa no computador que permitirá o acesso a qualquer momento desejado.

6.2.2 Ataque Distribuído de Negação de Serviço (DDoS)

Um ataque de negação de serviço (Denial of Service) tem como finalidade tornar os recursos de um sistema indisponíveis. Não se trata somente de invasão de sistemas e sim uma ação que provoca sobrecarga nos mesmos. Um ataque DDoS pode ser realizado por meio de uma rede de Botnet (ALMADA, 2013, p 40). Uma botnet é uma rede composta por um conjunto numeroso computadores infectados por um malware que sequestra as máquinas e as converte em “bots” (robôs ou zumbis), ficando submetidos ao controle de um hacker. Quanto maior a botnet, mais poderosa ela é. O DDoS pode ser entendido através do exemplo apresentado por Pasini:

> “ Esse ataque consiste em comandar, pela rede, vários computadores de usuários conectados a internet, sem que estes percebam, para acessar simultaneamente uma determinada página na internet, sobrecarregando o servidor da instituição dona deste *site* e, assim, fazendo com que ele pare de funcionar por algumas horas ou dias. Poderá ser gravíssimo ao derrubar-se, por exemplo, o *site* da Receita Federal na última semana de declaração do imposto de renda.” (PASINI, 2012, p. 38).

Esse ataque foi realizado pela Rússia contra sites do governo, de agências bancárias e de sistemas de energia elétrica da Estônia. Essa ação foi repetida em 2008, quando a infraestrutura de internet da Geórgia foi derrubada durante o conflito com a Rússia. (PASINI, 2012 p. 33).

Do acima exposto, percebe-se que qualquer sistema de comando e controle centrado em redes é passível de sofrer ataque de uma botnet, principalmente se estiver conectado à Internet.

6.2.3 Injeção de Linguagem de Consulta Estruturada

Trata-se de uma técnica é usada para roubar informações (senhas, dados financeiros, etc) ou para dar ao hacker o controle não autorizado de um servidor, enganando sistemas de segurança, permitindo o controle sistemas, principalmente os de infraestruturas críticas, à distância. Essa técnica de invasão de um site de serviços, como o bancário, consiste em inserir um comando malicioso no código do sistema, que normalmente usa uma forma de programar denominada de *Structured Query Language* (SQL), sigla em inglês. Foi a tática que permitiu o furto de dados dos usuários da rede do PlayStation por parte do grupo LulzSec. (FERRARI et al., 2011, p. 94, apud PASINI, 2012, p. 38):

6.2.4 Os atores que ameaçam o espaço cibernético

Os atores mais perigosos no domínio cibernético ainda são os Estados-Nação, apesar das crescentes capacidades das organizações e dos grupos irregulares ou criminosos. Os atores não estatais necessitam da conivência dos governos para que tenham plena liberdade para explorar ao máximo suas capacidades e motivações. Pode-se afirmar que, com a direção Estatal, obtem-se os efeitos desejados das ações de G Ciber realizadas por todos os atores de forma racional. Assim, sem

coordenação do Estado os atores irregulares deixam de ser importantes parceiros na busca pela superioridade da informação.

Conforme afirma Pinheiro (2008, p. 6), organizações revolucionárias não estatais, integradas por forças irregulares, vêm empregando a Tecnologia da Informação em Conflitos de 4ª Geração, dela extraindo vantagem considerável. Isso revela o protagonismo desses atores nos conflitos atuais.

Verifica-se a tendência de que cresçam as possibilidades de ataques perpetrados não só por Estados, mas também por organizações ou por forças irregulares. São grupos de hackers que podem ser explorados ou recrutados por Estados, por meio de elementos de Inteligência ou Forças Especiais, para desempenharem atividades de interesse tático, operacional ou estratégico em operações de informação.

6.2.4.1 Grupos de Hackers

Os diversos grupos hackers adotam condutas distintas. Podem ser pacíficos, como os que cooperam para o desenvolvimento de software livre, da inclusão digital ou da segurança da informação. Podem também ser ilícitos (crackers ou criminal hackers), como os que quebram códigos e invadem sistemas por motivação ideológica ou criminosa, onde se enquadram os fraudadores, ciber-terroristas e hackerativistas. Afirma-se que um hacker é a melhor arma para combater o cracker. Isso ficou claro por ocasião da prisão do craker Kevin Mitnick[4], capturado pelo FBI com ajuda de hackers. Do exposto, é importante estudar as capacidades de alguns exemplos notáveis de grupos de hackers ilegais como o Anonymous, o LulzSec e a Rede de Negócios Russa.

O Anonymous é a face mais conhecida do universo hackerativista atual. É um movimento que reúne ativistas de várias matizes ideológicas. O grupo ganhou notoriedade em 2008 defendendo a liberdade de expressão na Internet, porém já demonstrou de capacidade de desestabilizar sistemas corporativos. Em fevereiro de 2012, uma fração brasileira do Anonymous atacou os sites do Banco Central e dos bancos BMG, Citibank e Pan Americano, que ficaram temporariamente instáveis. O

[4] Kevin David Mitnick é um hacker norte-americano que ficou conhecido mundialmente a partir dos anos 90. Atualmente trabalha como gerente de uma empresa de segurança.

grupo assumiu a autoria de ataques aos sites dos bancos Itaú, Bradesco, Banco do Brasil e HSBC, ocorridos no mesmo período (PASINI, 2012, p. 64).

O LulzSec é um grupo emergente no universo hacker. Trata-se dos elementos que tiraram do ar por três semanas a rede on-line do PlayStation, da Sony, e obtiveram informações confidenciais de 77 milhões de usuários. O grupo reivindicou ataques a sites ligados ao governo americano. A página da Agência Central de Inteligência (CIA) ficou fora do ar por horas e dados de usuários do site Senado norte-americano foram roubados. O grupo se considera paladino da justiça, empenhado a expor ao povo a corrupção pela difusão de informações extraídas dos sistemas do governo e assim obter apoio popular para suas causas e repercussão de suas ações na imprensa.

A Rede de Negócios Russa é considerada a principal organização mundial no fornecimento de suporte a ciberataques por parte do crime organizado. O grupo não possui perfil ativista e controla um grande número de *botnets, capazes de r*ealizar negação de serviço por força bruta. O emprego de *bots contra a Geórgia em 2008 aponta para o* envolvimento do crime organizado russo, seja diretamente, pelo lançamento de ataques de negação de serviço, ou de forma indireta, pelo “aluguel” de suas *botnets* para grupos patrióticos. O fato de sítios *hacktivistas* (como o StopGeorgia.ru) estarem vinculados ao crime organizado russo e terem feito uso de botnets fundamenta tal hipótese (SHAKARIAN, 2011, p. 71).

6.3 EMPREGO DA GUERRA CIBERNÉTICA EM OPERAÇÕES DE INFORMAÇÃO

As Op Info consistem em um trabalho coordenado, metodológico e integrado de capacidades relacionadas à informação, em conjunto com outros vetores, para informar e influenciar grupos e indivíduos, bem como afetar o ciclo decisório de oponentes mantendo a proteção sobre as próprias informações.

> “ As Operações de Informação visam evitar, impedir ou neutralizar os efeitos das ações oponentes na Dimensão Informacional. Integram capacidades relacionadas às atividades de Comunicação Social, Operações Psicológicas, Guerra Eletrônica, Guerra Cibernética, para contribuir para a obtenção da Superioridade de Informações.” (BRASIL, 2013, p 14)

A guerra cibernética é um dos sete vetores da Guerra da Informação, a qual também engloba a guerra eletrônica e outros vetores conforme apresentado na Figura 23.

Figura 23 - Sinergia das operações de informação

Fonte: Carneiro (2012)

6.3.1 A Integração das Ações Cibernéticas e de Guerra Eletrônica

Normalmente, as ações cibernéticas e eletromagnéticas são atividades desenvolvidas para apreender, reter e explorar uma vantagem sobre oponentes ou potenciais adversários, tanto no espaço cibernético como no espectro eletromagnético e, simultaneamente, negar e degradar ao adversário a utilização dessa vantagem e proteger o nosso processo decisório, particularmente o sistema de comando e controle.

Esses vetores se apoiam mutuamente e a integração das referidas capacidades são um facilitador, uma vez que contribuem para afetar a percepção e a tomada de decisão do adversário. Isso permite que elementos da F Ter garantam e mantenham a liberdade de ação no espaço cibernético e no espectro eletromagnético para nossas forças, enquanto buscam explorá-la ou negá-la aos oponentes. (BRASIL, 2014b).

A prática dessa integração fomenta estudos doutrinários no Exército Brasileiro para a estruturação do Batalhão de Guerra Eletrônica, criado pela Portaria nº 351, Comandante do Exército, de 20 de maio de 2013. A OM deverá ser composta por subunidades de GE e de G Ciber. A OM é voltada para apoiar as ações da FTC no nível tático, sendo apta para atuar contra sistemas de controle da AAAe.

6.4 A GUERRA CIBERNÉTICA NO APOIO AO PODER AÉREO

Na grande maioria dos conflitos, a primeira fase da Batalha Aérea (Fase 1) é caracterizada pela busca da Superioridade Aérea (Sp Ae). Os objetivos prioritários para a conquista e a manutenção da Sp Ae são as aeronaves, os aeródromos, os órgãos de comunicações, controle e alerta do sistema de D Aepc, os meios de defesa antiaérea e a indústria aeronáutica (BRASIL, 2001, p. 1-1).

A atuação cibernética, seja operacional ou tática, é tipicamente empregada no contexto de uma operação militar. Tem foco na preparação do campo de batalha, visando apoiar uma ação militar de forma sincronizada com a manobra (BRASIL, 2014e, p. 23). Isso reforça a possibilidade de emprego de vetores das Operações de Informação com a finalidade de silenciar defesas antiaéreas durante a 1ª fase da batalha aérea.

Segundo a doutrina da FAB, a Tarefa de Superioridade Aérea visa a objetivos específicos do poder aeroespacial inimigo. As defesas antiaéreas, os centros de controle, os meios de detecção e de telecomunicações da defesa aeroespacial estão incluídos entre os alvos típicos a serem atacados. Essa tarefa representa a mais alta prioridade para a Força Aérea, onde está incluída a missão de Supressão de Defesa (BRASIL, 2005, p. 34).

> “ Supressão de Defesa. Missão Aérea destinada a destruir, neutralizar ou degradar a capacidade de defesa aérea e de C² inimigo, em determinada área e por um período de tempo, usando energia eletromagnética ou armamento que empregue a emissão intencional do alvo para o seu guiamento.” (BRASIL, 2005, p 36).

Pode-se admitir que os sistemas de AAAe são alvos que certamente serão buscados por forças aéreas e cibernéticas adversas. A G Ciber pode ser usada em conjunto com medidas de ataque de GE no apoio a missões aéreas de ataque. Já existem estudos acadêmicos na FAB voltados para essa alternativa de emprego das ações cibernéticas. Segundo Da Veiga (2012, p.7), no âmbito da FAB o ataque cibernético representa as atividades de Def Ciber ofensivas que empregam meios de Força Aérea para neutralizar ou destruir os SCTIC² inimigos.

De acordo com Carneiro (2012, p. 151) o Dst Cj G Ciber pode realizar ações de ataque cibernético, colaborando com o esforço de interdição e com a conquista da superioridade aérea, em alvos de interesse do TO.

No caso da intervenção militar ocorrida na Líbia (*Operação Odyssey Dawn*), especialistas militares norte-americanos analisaram formas de usar a cibertecnologia para desativar sistemas de comunicações e de radares aéreos líbios, antecedendo os ataques aéreos da OTAN (FINK e col., 2014, p. 42).

Estima-se que a possibilidade de um confronto dos EUA com o Irã ou a Síria tem forçado os militares a avaliar o emprego de ciber-armas contra importantes alvos, tais como os sistemas de defesa aérea, mesmo que não estejam ligados as redes acessíveis pela Internet.

6.4.1 A Operação Orchard

Veiculou-se na imprensa que uma bateria antiaérea síria foi neutralizada em decorrência da contaminação de seus computadores por vírus. Isso teria ocorrido por causa da contaminação dos computadores durante ataque aéreo realizado por Israel, conforme exposto pela historiadora Fernanda Corrêa. Israel, objetivando destruir a usina nuclear síria de Al Kibar, promoveu um ataque aéreo conhecido como Operação Orchard. A Síria dispunha de um sofisticado sistema de defesa antiaérea russo. Israel teria alterado o referido sistema para que este não visualizasse os caças israelenses. Acredita-se que Israel tenha se utilizado de neutralização remota. O ciberataque foi possível graças ao fato de um comissário sírio ter seu notebook hackeado pelo serviço secreto de Israel. Embora a Síria acuse Israel, o governo judeu nega a autoria do ataque aéreo e do ataque cibernético (CORREA, 2013).

6.5 O ESPAÇO CIBERNÉTICO BRASILEIRO E SUAS FRAQUESAS

A política de Segurança Cibernética no Brasil é recente. Pode-se afirmar que teve início de fato a partir de 2008, após a aprovação da Estratégia Nacional de Defesa. Antes disso, o país já se constituía um terreno fértil para a atuação das ameaças cibernéticas, o que ainda se observa na atualidade.

Em 2006, a China foi responsável pela produção de 30% dos *softwares* maliciosos, sendo a maior no mundo. O Brasil foi o segundo maior, com responsabilidade de cerca de 14%. Isso foi divulgado pelo Núcleo Operacional da Sociedade da Informação no Brasil (MANDARINO JUNIOR e CANOGIA, 2009, p.36).

Conforme pesquisa realizada pela empresa Módulo Security, em 2007, 31% das organizações não sabem informar se sofreram ou não tentativas de invasão, das falhas de segurança ocorridas, 24% são causadas por funcionários da própria organização. Conclui-se que o maior obstáculo para a implementação de medidas de segurança preventivas é a falta de conscientização de todos os usuários, que mesmo possuindo conhecimento sobre as normas e legislação específicas, resistem em cumprí-las. Mandarino Júnior (2009, p.143) reforça a conclusão da referida pesquisa. O mesmo afirma que a cultura da segurança da informação e comunicações é incipiente em órgãos e entidades da administração pública federal.

Em 2009 o Brasil já possuía 320 grandes redes corporativas. A EBNET é um dos exemplos. Naquele ano essas redes sofreram dois mil ataques por hora (MANDARINO JUNIOR, 2009).

Verifica-se que a preocupação com a segurança cibernética é pouco valorizada na sociedade brasileira, confirmando que o espaço cibernético do Brasil é atrativo para o desenvolvimento de ações hostis de G Ciber.

6.5.1 O Espaço Cibernético Brasileiro atual.

O Brasil é o país mais populoso da América Latina com mais de 200 milhões de habitantes. A participação de usuários de Internet é de quase 88,5 milhões desde 2011. Duas em cada cinco famílias brasileiras (38%) já têm acesso à Internet. Mais de 13% dos usuários contam Internet de banda larga com velocidades acima de 4 Mbps. O Brasil também tem o terceiro maior mercado de computadores, o quarto maior mercado de telefones celulares.

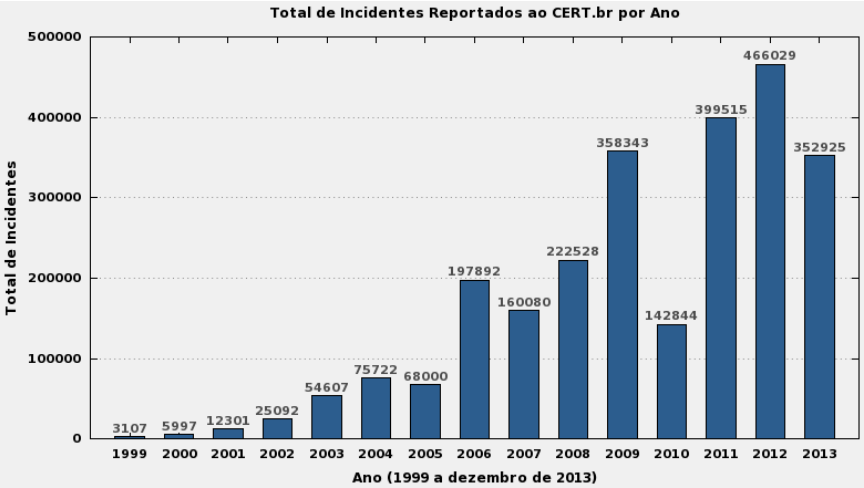
No Brasil, ainda não se tem notícia oficial de ataques cibernéticos efetuados com finalidade precípua de degeneração de sistemas estratégicos. Especulou-se que o chamado apagão elétrico, ocorrido no final de 2009, tenha sido ocasionado, por ataques cibernéticos, o que, efetivamente, não foi comprovado. No entanto isso não é certeza de que as infraestruturas críticas do país não estão vulneráveis.

Recentemente o Governo Brasileiro foi espionado pelos órgãos de inteligência dos Estados Unidos, incluindo a Presidente do Brasil Dilma Rousseff, que teve seu sigilo telefônico e virtual violados. A informação foi proveniente do Sr. Edward Snowden, ex-analista da Agência de Segurança Nacional (NSA, sigla em inglês) dos EUA.

No Brasil existem poucos analistas de carreira específica em segurança cibernética. Além disso, na maioria dos órgãos do governo são reduzidos os recursos financeiros previstos em orçamento destinado à segurança cibernética.

O Brasil apresenta o maior número de internautas da América Latina, cerca de 40 milhões ou 20% do total. A quantidade de incidentes reportados em 2012 totaliza 466.029. Isso representa um aumento superior a 1.800% no último decênio. O Comitê Gestor da Internet no Brasil divulgou por meio do CERT.br[5] (2013) as estatísticas de incidentes na Internet que foram reportados até 2013. Dados relevantes podem ser verificados na Figura 24.

Figura 24 – Incidentes reportados



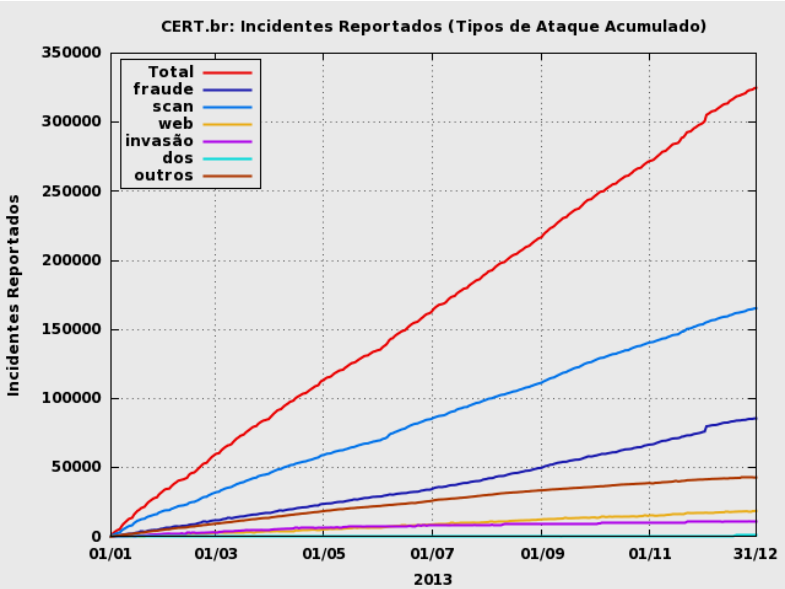
Fonte: Cert.br (2013)

Em relação aos ataques a servidores Web ocorridos em 2013, o Comitê observou uma grande quantidade de notificações de ataques de força bruta contra sistemas de gerenciamento de conteúdo. Os ataques foram, na maioria, tentativas de adivinhação das senhas das contas de administração destes sistemas. Em geral

[5] Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. É o Grupo de Resposta a Incidentes de Segurança para a Internet brasileira, mantido pelo NIC.br, do Comitê Gestor da Internet no Brasil. É responsável por tratar incidentes de segurança em computadores que envolvam redes conectadas à Internet brasileira.

os atacantes exploram vulnerabilidades em aplicações Web para, então, hospedar nesses sites páginas falsas de instituições financeiras. Observa-se que o perfil da maioria dos ataques é criminoso, sendo ainda raros os ataques de negação de serviço (DoS), conforme se verifica na Figura 25, na linha azul mais clara.

Figura 25 – Tipos de ataques



Fonte: Cert.br (2013)

6.5.2. Vulnerabilidades do Espaço Cibernético Brasileiro

As vulnerabilidades existentes no espaço cibernético brasileiro advém principalmente da dependência tecnológica em relação a países com alto grau de desenvolvimento na área da Tecnologia da Informação e Comunicações, problema que dificilmente será superada em curto prazo. Outra, já citada, resulta da falta de consciência a respeito da necessidade de se proteger informações sensíveis. Destaca-se também a falta de regulamentação do uso do espaço cibernético no Brasil. Essas fraquezas foram apontadas em audiência pública ocorrida no Senado Federal em setembro de 2013.

> “Agrega-se às vulnerabilidades citadas anteriormente, o escasso arcabouço legal nacional e internacional, que motivou o regime de urgência na tramitação do Marco Civil da Internet e tem marcado a posição do nosso País na necessidade de se discutir o estabelecimento de um marco regulatório também no plano internacional, principalmente após o caso Snowden.” (BRASIL, 2013).

6.5.2.1 As Vulnerabilidades que Afetam as Forças Armadas

A realidade da Marinha do Brasil pode ser considerada um espelho do ocorre em algumas unidades das demais Forças Armadas. De acordo com Pinto (2009), o conjunto de vulnerabilidades levantadas na Marinha do Brasil que afetam os sistemas de informação face às ameaças cibernéticas é decorrente de diversos fatores dos quais se destacam:

> "1) Falta de conscientização quanto ao problema, suas ameaças e riscos;
> 2) Escassez de incentivos à pesquisa e desenvolvimento de tecnologia própria nacional em dispositivos e procedimentos voltados à Segurança da Informação;
> 3) Escassez de suporte em pesquisa acadêmica na área de defesa cibernética, incluindo pesquisa nacional em criptologia;
> 4) Utilização de sistemas totalmente importados e com tecnologia proprietária, "caixa-preta";
> 5) Falhas de segurança nos protocolos, sistemas operacionais e aplicativos utilizados e que não são devidamente corrigidos;
> 6) Privatização total, sob o controle de empresas estrangeiras, da infraestrutura crítica nacional de telecomunicações;
> 7) Inexistência de políticas, normas e certificações voltadas à defesa ante as ameaças de GC; e
> 8) Inexistência de procedimentos de segurança e planos de contingência.devidamente testados, mostrando que a cultura de segurança é heterogênea e incipiente."(PINTO, 2009, p. 33) .

As mídias virtuais hoje existentes, como Blogs, Facebook emails, etc, em virtude da grande capacidade de banda larga na Internet, são empregadas para transmitir mensagens e fotos e vídeos. Quando associadas aos fatores acima mencionados, essas mídias podem contaminar redes militares como a EBNET.

Segundo Pasini (2012, p. 84) as redes que não devem estar acessíveis a partir da Internet, redes privadas (intranet), podem ser invadidas pelos equipamentos wireless ou contaminadas por malwares transportados em pen-drives.

6.6 MEDIDAS DE PROTEÇÃO CONTRA AMEAÇAS CIBERNÉTICAS

Enfrentar ameaças cibernéticas significa proteger três dimensões: a física, a informacional e a cognitiva. Os ataques cibernéticos são direcionados, em sua maior parte, para as dimensões física e informacional, ou seja, contra equipamentos e softwares. A proteção física permite impedir ou minimizar os efeitos de ataques à

infraestrutura. A proteção informacional visa deter ataques diretos ou indiretos. Os ataques diretos são prevenidos por meio de tecnologias que estão na interface entre as dimensões física e informacional. As possibilidades de ataques indiretos podem ser minimizadas desenvolvendo softwares seguros. Para tanto, se faz necessário normatizar sistemas e capacitar o elemento humano. A proteção da dimensão cognitiva está em defender o elemento humano e sua capacidade de decisão.

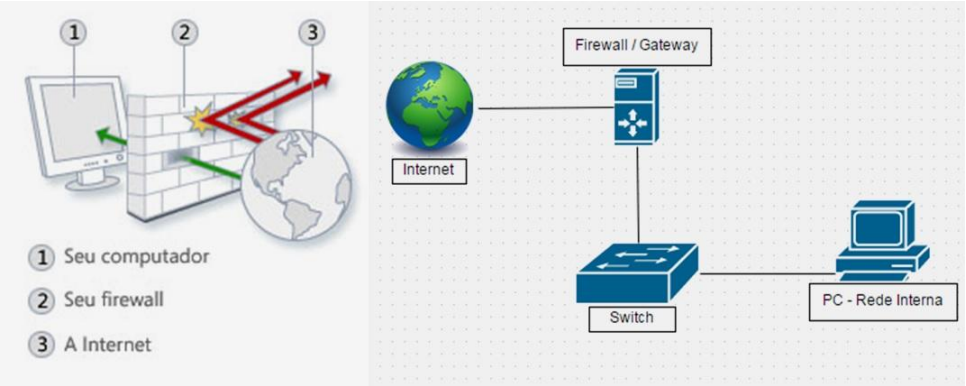
6.6.1 Protegendo as Dimensões Física e Informacional

O Firewall, o controle de acesso e o antivírus são formas básicas de reduzir significativamente a exposição a riscos. Além de firewalls e proteção antivírus, a educação também é importante (PASINI, 2012, p. 64). Existem outras medidas de defesa normalmente encontradas em sistemas de informação como Virtual Private Network (VPN), Anti-Spyware, sistemas de detecção de intrusões (IDS), ferramentas de gestão de vulnerabilidades e patch, filtragem web/URL (Proxy), máquinas virtuais, criptografia e sistemas biométricos.

6.6.1.2 Firewall

O *firewall* é um software instalado em um hardware destinado para verificar informações provenientes da Internet ou de outra rede, e as bloqueia ou permite que elas cheguem ao terminal do usuário, de acordo com as configurações estabelecidas pelo administrador, conforme ilustrado na Figura 26.

Figura 26- Firewall



Fonte: Microsoft Corporation, modificada pelo autor.

A filtragem pode ocorrer baseada em parâmetros como porta lógica, endereço de origem, destino, estado da conexão. Funciona através da comparação de regras para saber se um código tem ou não permissão para passar por determinada porta. Um firewall pode ajudar a impedir que hackers ou malwares obtenham acesso ao computador através de uma rede ou da Internet e também impede que um computador contaminado contamine outros terminais de uma rede. (MICROSOFT, 2015). No mundo cibernético, onde a distâncias não fazem diferença, a robustez do sistema de *firewall adotado pela* corporação passa a ser a linha de fronteira.

6.6.1.3 *Bridge com Firewall*

Uma forma mais elaborada de aplicar o uso de Firewall e que pode ser aplicada na proteção da EBNET no nível de nós de acesso, ou seja, no nível OM, é o uso da *Bridge* com *firewall. É uma solução* de baixo custo e baseada em Software livre. A solução é instalada em cada centro conectado diretamente ao *backbone* da rede corporativa. A *Bridge* com *firewall* tem as funções de firewall, detecção de intrusão e de *Proxy.* Pode também segmentar a rede dividindo-a em três sub-redes, isolando terminais por necessidades de acesso e de serviços. As sub-redes podem ser externa, interna e DMZ[6]. A rede externa é a não pertence à organização, como o exemplo da EBNet. A DMZ contém poucas máquinas com serviços que precisam estar acessíveis pela EBNet. A rede interna é composta por equipamentos sem necessidade de acesso a rede externa. (MENDONÇA, 2007, p. 3).

Softwares abertos (open source) podem ser usados nas funções de Bridge Firewall. São exemplos: Detector de Intrusos Snort, Serviço Proxy Squid e a Ferramenta de Análise de Tráfego Ntop. Dessa forma, é possível fazer uma monitoração e gerência completas sobre o tráfego de rede através de gráficos e imagens (MENDONÇA, 2007, p. 8).

[6] Zona desmilitarizada. É uma sub-rede física ou lógica que contém e expõe serviços de fronteira externa de uma organização a uma rede maior e não confiável, normalmente a Internet. A função de uma DMZ é manter todos os serviços que possuem acesso externo juntos em uma rede local, limitando assim o potencial dano em caso de comprometimento de algum destes serviços por um invasor.

6.6.1.4 Antivírus

Os antivírus são programas que procuram detectar e, então, anular ou remover os vírus de computador. Atualmente, novas funcionalidades têm sido adicionadas aos programas antivírus, de modo que alguns procuram detectar e remover cavalos de tróia, barrar programas hostis e verificar e-mails. O antivírus monitora automaticamente todos os arquivos que são abertos no PC. O código de computador que compõe cada um deles é comparado com a coleção de vacinas, que nada mais é do que um acervo com pedaços do código dos vírus. Se um arquivo tiver trechos similares aos de um vírus, está contaminado, o antivírus poderá tentar restaurar o arquivo original, podendo também isolar ou eliminar o arquivo afetado se necessário. Um antivírus não é capaz de impedir que um atacante tente explorar alguma vulnerabilidade existente em um computador, não sendo eficaz contra o acesso não autorizado a um backdoor instalado em um computador.

Os programas antivírus são efetivos somente se receberem constantes atualizações. Para isso ser garantido, é necessário que existam desenvolvedores comprometidos com o software. Sendo o código do antivírus de domínio nacional acredita-se que será mais confiável.

O Exército Brasileiro coordena a compra de antivírus para uso nas suas OM, a fim de padronizar de um único *software* de segurança cibernética para os sistemas informatizados da Força, usando com requisitos únicos para a Instituição. Coube ao Centro de Desenvolvimento de Sistemas (CDS) apresentar as especificações do software. Trata-se de uma solução de antivírus corporativo multiplataforma para servidores e estações de trabalho com gerência centralizada, com direito de atualização de 36 meses. O software AvWare Defesa BR deverá ser nacional com capacidade de proteger os 60 mil computadores do Exército Brasileiro (BRASIL, 2015a).

O valor estimado do projeto é de R$ 720 mil. Está em fase de desenvolvimento na empresa Blue Pex em parceria com especialistas do EB. Sendo o código do antivírus de uso exclusivo do EB, haverá dificuldade por parte de possíveis atacantes descobrirem os pontos fracos do programa em curto prazo, o que dificulta o desenvolvimento de armas cibernéticas em tempo oportuno.

6.6.1.5 Sistemas de detecção de instrução

Os sistemas automáticos de detecção de ataques (intrusion detection systems, IDS) servem para detectar anomalias no sistema e identifica os modelos de agressão conhecidos. Habitualmente, os IDS operam em combinação com os IRS (intrusion response systems - sistemas de resposta de intrusão), cujas medidas costumam consistir na desconexão total ou parcial do sistema ou o reparo automático de danos.

6.6.1.6 Servidor P*roxy*

O servidor *proxy* atua como procurador do cliente na navegação *Web,* intermediando a conexão entre as máquinas da rede local e a rede externa (Internet). O emprego de *proxy* tem a grande vantagem de permitir o armazenamento local dos conteúdos mais frequentemente utilizados. Desta maneira, quando um usuário acessa uma página que ficou armazenada no *proxy*, ele não apenas a recebe com uma velocidade muito superior se comparada com o acesso normal como, também, reduz o tráfego nos canais de comunicação.

6.6.1.7 Central Unificada de Gerenciamento de Ameaças

A UTM (*Unified Threat Management*) é uma solução integradora criada para segurança de redes e que vem se tornando a solução mais procurada na defesa de organizações. A UTM é teoricamente uma evolução do firewall tradicional, unindo a execução de várias funções de segurança em um único dispositivo (Figura 27): firewall, prevenção de intrusões de rede, antivírus, Virtual Private Network (VPN), filtragem de conteúdo, balanceamento de carga, geração de relatórios informativos e gerenciais sobre a rede.

Figura 27 - Central Unificada de Gerenciamento de Ameaças

Fonte: Bluepex

6.6.1.8 Redes Ponto a ponto (*ad-hoc*)

As redes ad-hoc é uma forma menos vulnerável de utilizar redes Wireles, pois não utiliza ponto de acesso (access point), onde passa todo o fluxo de informações da rede. Assim, um pequeno grupo de máquinas pode se comunicar entre si diretamente, o que permite que a rede fique mais restrita. Os computadores da rede funcionam como se fossem um roteador, substituindo o ponto de acesso, encaminhando informações oriundas vêm de dispositivos vizinhos. Este tipo de rede permite flexibilidade e mobilidade aos terminais da rede.

6.6.1.9 Algoritmos de Criptografia e de Criptofonia

Atualmente o uso da criptografia nos sistemas que exigem sigilo e proteção é imprescindível, particularmente na Internet, onde existem home-bankings. Por esse motivo foi criada a Rede Nacional de Segurança da Informação e Criptografia (RENASIC) em 2008. A criptografia digital é o que garante que informações confidenciais sejam enviadas e processadas em meios não confiáveis. Nos meios de comunicações pouco seguros os programas criptográficos devem ser associados a outras aplicações para proteger de dados. A criptografia digital garante privacidade, autenticidade e integridade da informação nos sistemas centrados em redes.

A criptografia pode ocorrer por chave simétrica (chave única) ou assimétrica (duas chaves). O nível de segurança de uma criptografia é medido no número de bits, ou seja, quanto mais bits forem usados, mais difícil será quebrar a criptografia. São exemplos de métodos criptográficos que usam chave simétrica: AES, Blowfish, RC4, 3DES e IDEA.

A criptografia de chave simétrica, quando comparada com a de chaves assimétricas, é a mais indicada para garantir a confidencialidade de grandes volumes de dados, pois seu processamento é mais rápido.
Um exemplo prático do uso de algoritmos de criptografia para proteger o tráfego de dados nas Internet são as Redes Privadas Virtuais (VPN).

As técnicas de criptofonias são utilizadas para transformar um sinal de voz em sinal ininteligível com o propósito de evitar escutas não autorizadas. Já existem equipamentos de criptofonia digital. É uma tecnologia que demanda maior largura de banda para transmissão. São úteis nos sistemas de comunicações móveis, particularmente se associados à RDS, pois estes não requerem grandes adaptações e substituições no hardware. São algoritmos que empregam Codificadores/Decodificadores (CODECs).

6.6.2 O Fator humano e a proteção da Dimensão Cognitiva.

O recurso humano é elemento fundamental na proteção contra as ações de G Ciber. O sucesso da segurança da informação reside no treinamento, na capacitação e na conscientização dos usuários e administradores de sistemas.
Uma das ações emergenciais a serem adotadas no Brasil é a capacitação, em maior escala, de profissionais, por meio da futura Escola Nacional de Defesa Cibernética (SENADO FEDERAL, 2013, p. 6).

Segundo Carneiro (2012, p. 124) um dos aspectos limitadores da defesa cibernética é a dificuldade de identificação de talentos humanos. Assim, é necessário buscar formas de aumentar o efetivo de especialistas no âmbito do setor cibernético de defesa. Em relação a esta problemática o General de Brigada Álvaro Pinheiro assim expôs sua preocupação:

> “A elevação do Brasil a patamares adequados passa por um maior incentivo à formação acadêmica de recursos humanos especializados em: resposta a incidentes; verificação de vulnerabilidades; teste e correção de procedimentos e, onde há que se enfatizar, redução da dependência externa e diferentes áreas de pesquisa. Em termos de criptografia nacional, é impositivo o desenvolvimento de códigos nacionais, o incremento das atividades de criptoanálise e a regulamentação de códigos e auditorias.” (Pinheiro, 2008, p. 10)

O elevado grau de complexidade dos dispositivos modernos de comando e controle e das tecnologias de segurança de redes exige a presença de especialistas capazes de atuar de imediato sobre os incidentes de segurança ou de funcionamento. Os sistemas militares operam quase sempre 24 horas nos sete dias da semana, o que representa uma dificuldade em dispor de um efetivo de especialistas compatível. Isso pode impor a necessidade dos alguns órgãos de C² terem que buscar a proximidade física entre si, sempre que possível.

6.6.2.1 A Capacitação de RH em G Ciber e Op Info no EB

Para atender a demanda por especialistas, o Exército Brasileiro busca capacitar militares na área de Defesa Cibernética. Em 2010, o Centro de Instrução de Guerra Eletrônica (CIGE), centro de ensino subordinado ao Centro de Comunicações e Guerra Eletrônica do Exército, conduziu o primeiro Estágio de Defesa Cibernética para Oficiais e, posteriormente, para Cadetes da Academia Militar das Agulhas Negras. O CIGE tornou-se o responsável pela capacitação dos recursos humanos do EB na área de G Ciber. Nesse sentido, foi criado no Exército Brasileiro o Curso de Guerra Cibernética para Oficiais através da Portaria nº 24 do Estado-Maior do Exército, de 21 de março de 2012. Da mesma forma foi criado um curso similar para praças a ser conduzido pelo CIGE.

6.6.2.2 Treinamento de pessoal

Um aspecto importante no preparo do pessoal para o combate na G Ciber é a simulação de incidentes. É necessário que sistemas sejam desenvolvidos de forma que seja possível criar cenários simulados de ataques cibernéticos. São necessários que existam simuladores nos centro de C² mais críticos. Assim, será possível orientar e treinar pessoal para sanar incidentes também no nível tático.

6.6.2.3 Proteção e Controle dos Gestores de Rede

A segurança da informação passa pela segurança dos recursos humanos. Um dos maiores pontos fracos das redes é o pessoal com acesso administrativo aos servidores. Uma forma de ameaça que pode ocorrer quando o inimigo sequestra um

membro da família de um operador de rede e, em seguida, o força a instalar um *malware*. Esse é um motivo para as agências governamentais e empresas privadas que cuidam das infraestruturas críticas terem um adequado controle de segurança com seus empregados (PINTO, 2009 p. 15). Diante disso, é necessário que existam formas de evitar que elementos adversos tenham acesso a esses especialistas, pois, além disso, são de difícil recrutamento e substituição.

6.6.2.4 O Apoio em Pessoal do Dst Cj G Ciber aos Elementos Táticos

Segundo o previsto na Doutrina Militar de Defesa Cibernética, o Dst Cj G Ciber atua prioritariamente no nível operacional, possuindo algumas capacidades de apoio aos escalões componentes de um Comando Conjunto. Esse apoio ocorre da seguinte forma:

1) Identificando e analisando vulnerabilidades nas redes de computadores e aplicações empregadas nos Sistema de C² desdobrados na operação;

2) Recomendando ações para mitigar as vulnerabilidades identificadas; e

3) Estudando as ameaças e seu impactos nas redes de C² ou quaisquer outras estruturas ou recursos computacionais das forças amigas.

Conforme publicado na Revista Verde Oliva, durante a Operação Rio + 20 e a Jornada Mundial da Juventude, o Centro de Defesa Cibernética se limitou a monitorar as redes sem intervir diretamente nas mesmas, atuando de forma colaborativa com os demais órgãos na solução de incidentes ocorridos no espaço cibernético. Coube aos gestores das diversas redes envolvidas solucionar os incidentes em seus respectivos sistemas empregando seus próprios profissionais de TI (2014, p. 41).

Verifica-se que doutrinariamente o apoio prestado pelo destacamento aos elementos do nível tático fica limitado ao monitoramento das redes, às orientações e ao suporte técnico, o que deve ocorrer por canal técnico. Verifica-se que no caso da AAAe, não é previsto a presença de um especialista do destacamento no COAAe P. Assim sendo, é necessário que este centro de C² tenha um especialista próprio com capacidade seguir as instruções passadas pelo Dst Cj G Ciber principalmente nas situações de emergência.

6.7 O EXEMPLO DA FORÇA AÉREA BRASILEIRA

A FAB vem providenciando melhorias na segurança de seus sistemas de informação e comunicações. Podem ser citados os seguintes projetos desta força junto ao Ministério da Defesa, os quais podem servir de base para uma proposta no âmbito da Força Terrestre no que for julgado oportuno.

1) implantação de uma estrutura de gerenciamento para coordenar a implantação da segurança das informações dentro das organizações;

2) capacitação de recursos humanos na área de segurança da informação;

3) gerenciamento Eletrônico de Documentos – GED, que deverá estar de acordo com a Infraestrutura de Chaves Públicas Brasileira (ICP – Brasil);

4) instalação e manutenção de salas-cofre;

5) telefonia fixa segura;

6) proteção da telefonia celular;

7) certificação digital;

8) ativação de grupos de resposta a incidentes de segurança;

9) capacitação de recursos humanos na área de segurança da informação;

10) adequação das normas para aquisição, desenvolvimento e manutenção dos projetos e sistemas;

11) aquisição ou desenvolvimento de ferramentas de software capazes de identificar, alertar e responder automaticamente ao surgimento de problemas importantes; e

12) estabelecimento, de um grupo com capacitação específica para executar ações ofensivas contra um inimigo declarado.

Essas providências foram apresentadas ao MD por meio do ofício nº 3/6SC1, de 15 de abril de 2004, do Estado Maior da Aeronáutica. Observa-se que grande parte dos projetos pretendidos pela FAB estão alinhados com medidas cabíveis no EB para proteção contra ações cibernéticas hostis.

6.8 CONSIDERAÇÕES

Ao estudar o presente capítulo, verificou-se que existe uma grande variedade ferramentas e atores capazes de realizar ações de G Ciber hostis. Isso pode ocorrer a partir de outros continentes ou mesmo do espaço cibernético brasileiro, o qual se

encontra favorável à ação de hackers. Dessa maneira, foi possível identificar as ameaças empregadas na Guerra Cibernética capazes atuar diretamente nos meios de comando e controle de um centro de comando e controle de uma Bda AAAe.

Pode-se confirmar que os meios à defesa aeroespacial estão entre os alvos prioritários nas campanhas aérea e cibernética do inimigo, com os apoios já tradicionais da inteligência e da GE.

Em meios a diversas técnicas elaboradas de invasão, o pen-drive infectado tem sido uma das formas de acesso mais simples e tradicionais, o que desperta atenção também para medidas simples de segurança como remover ou desabilitar portas USB.

Observa-se também a necessidade de meios alternativos de fornecimento de energia elétrica aos sistemas de C², pois estes podem ser afetados indiretamente por ataques cibernéticos contra empresas geradoras e fornecedoras de eletricidade.

Apresentou-se uma variedade de tecnologias e equipamentos capazes de fazer frente a tais ameaças. No entanto, ainda há uma grande deficiência no Brasil quanto aos recursos humanos confiáveis e em quantidade, capazes de usar as complexas ferramentas disponíveis para proteger os sistemas de comando e controle críticos do poder militar. Isso inclui, particularmente, os sistemas de proteção baseados em software de código aberto e de desenvolvimento nacional.

Considerando que a melhor arma contra um Hacker é outro Hacker, é mister que se continue dando prioridade e urgência na formação e identificação de talentos nesse setor. Esses especialistas são capazes de desenvolver e integrar sistemas de comunicações centrados em redes de uma mais forças, aplicando adequadamente aos mesmos as medidas de proteção cibernéticas cabíveis, sem prejuízo da eficácia.

Pode-se considerar que tempo é outro inimigo do hacker, pois é um fator limitador. Isso porque um novo malware representa um projeto relativamente demorado, podendo levar meses para ser desenvolvido. Qualquer mudança nas características do alvo pode exigir um novo projeto de ameaça. Assim, verifica-se que uma forma de combater um agente ator cibernético ameaçador é fazê-lo desistir do ataque.

Com base nas informações já apresentadas é possível identificar o perfil exigido para os recursos humanos, bem como o conjunto de opções de material de comunicações e de TI que podem ser adotados na estrutura de G Ciber na proteção de um COAAe principal.

De acordo com o apresentado, pode-se concluir que a complexidade e a dos meios e técnicas de proteção dos meios informatizados de C² de um COAAe P revelam a necessidade de haver mudanças na atual estrutura de comando e controle da Bda AAAe do Exército Brasileiro.

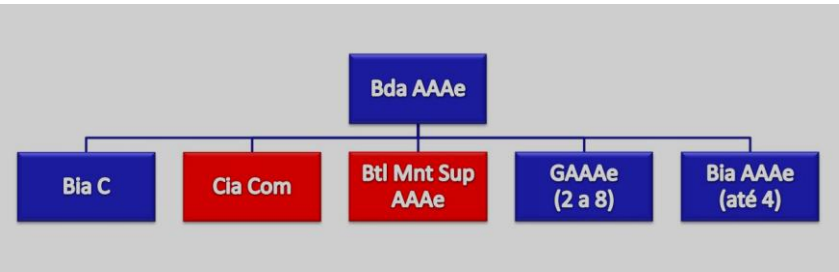
7. AS ATUAIS DEMANDAS ESTRUTURAIS DO COAAe DE BRIGADA DE AAAe

Ao estudar a atual organização do 1ª Bda AAAe verifica-se que a mesma não dispõe de uma companhia de comunicações diretamente subordinada, como ocorre em outras grandes unidades do Exército Brasileiro. Diante dessa carência, as tarefas de comando e controle ficam a cargo da Bateria Comando desta Bda, o que aponta para a necessidade de se buscar soluções que atendam às atuais necessidades do funcionamento do COAAe principal controlado pela Bda AAAe, elo fundamental na difusão de alerta, no acionamento coordenado da DA Ae e na execução de medidas de controle do espaço aéreo que envolvam os fogos antiaéreos.

7.1 A ATUAL ESTRUTURA DOUTRINÁRIA

Segundo a organização prevista na atual doutrina da AAAe, apresentada na Figura 28, uma Bda AAAe deve possuir uma Companhia de Comunicações (Cia Com), cujo Comandante possui o encargo de oficial de comunicações e eletrônica (O Com Elt) da Bda. Ficará a cargo desta SU estabelecer as ligações do COAAe P com os COAAe S, incluindo os COAAe S dos aos sistemas AAAe de média altura. O COAAe S receberá do COAAe P as medidas de coordenação da defesa antiaérea, como corredores de segurança, estados de alerta, estados de ação.

Figura 28 – Organograma da Bda AAAe



Fonte: BRASIL (2011b)

O Com Elt integra o EM especial da Bda, devendo participar de todo o planejamento dos aspectos das comunicações. Esta função também planeja, coordena e supervisiona a segurança das Com e os aspectos de GE do ramo das comunicações (BRASIL, 2001, p. 9-6). Pode-se constatar a importância desta função uma vez que:

> “A AAAe possui extrema vulnerabilidade às ações de guerra eletrônica (GE) inimigas, que terão ampla possibilidade de atuar sobre o sistema de controle e alerta e sobre o sistema de comunicações, e que, uma vez obtendo sucesso, degradarão significativamente a eficácia da AAAe.” (BRASIL, 2003, p 1-3)

A doutrina também prevê a função de oficial de guerra eletrônica dentro do EM da Bda AAAe, voltado para os aspectos GE de não comunicações (NCom). Na Bda AAAe caberá ao oficial de guerra eletrônica (OGE) do EM, ou ao E2, no caso da não existência do primeiro, a assessoria e o planejamento das ações de GE a serem executadas pelos escalões de AAAe subordinados referente ao controle sobre as emissões eletromagnéticas dos radares (BRASIL, 2003, p. C-2). Diante disso, verifica-se que, com base na doutrina de Op Info vigente, é possível que estruturas de GE desenvolvam capacidades em apoio à G Ciber.

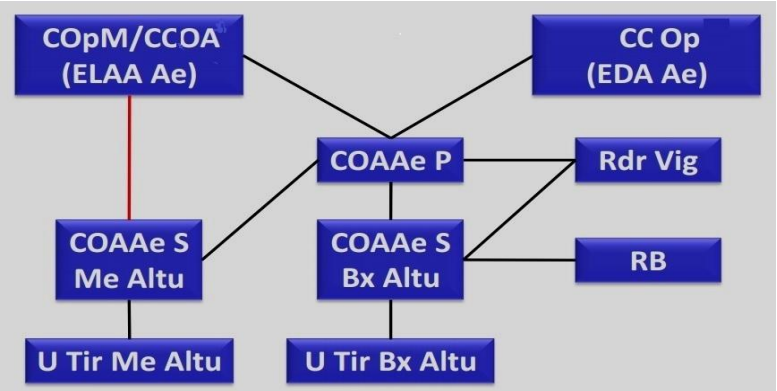
Em relação à organização da Cia Com, cabe ao Pel Com PC integrar a Bda ao sistema de comunicações via satélite ligado a um SISTAC de uma FTC desdobrada na área defendida pela Bda AAAe. Para isso, o Pel Com PC utiliza-se de uma Turma Rádio-Satélite. (BRASIL, 1998, p. 3-7).

7.1.1 Comando e Controle da AAAe de Média Altura

A doutrina vigente prevê GAAAe ou Bia AAAe de Me Altu subordinadas comando da Bda AAAe. As DA Ae empregadas contra aeronaves e mísseis nas faixas de emprego de média altura (entre 3000 e 15000 metros) utilizam apenas mísseis antiaéreos, dividindo o espaço aéreo com as aeronaves de interceptação. Devido a isso, terão seu emprego e seus fogos controlados e coordenados diretamente por centros de controle da Defesa Aérea (OCOAM do COpM ou do CCOA da FAC). Nesse caso, é indispensável à existência de comunicação direta da D Ae com o COAAe S, pois caso contrário, a DAepc poderá ficar seriamente comprometida por não permitir a coordenação do fogo frente a um ataque de uma ameaça aérea no tempo oportuno (BARROSO, 2004, p. 106).

As ligações mais rotineiras do COAAe P no TO são apresentadas na Figura 29. Observa-se a linha vermelha em destaque referente à ligação direta entre a AAAe de Me Altu e o COpM ou CCOA. Na ZI, normalmente não é necessário ligar-se com o CC Op da FTC.

Figura 29 - Fluxos de informações e ligações comuns do COAAe



Fonte: BRASIL (2011b)

7.2 A ATUAL ESTRUTURA EXISTENTE PARA ATENDER AS DEMANDAS DE C²

Conforme já observado, a Bda AAAe ainda não dispõe de uma Cia Com. Atualmente cabe à Bia C da Bda AAAe, todos os encargos de C² da Cia Com. Para isso, a Bia C possui em sua organização uma seção de comunicações, um destacamento de operações antiaéreas e uma seção de comando. Caberá ao Cmt desta Bia, acumular as atribuições de O Com Elt. O COAAe da Bda é desdobrado pelo destacamento de operações antiaéreas, enquanto o Posto de Comando é encargo da Seç Cmdo.

No organograma da Bia C em vigor, não existem militares voltados diretamente para as atividades de GE. As Cia Com orgânicas de Bda de Infantaria também não possuem previsão de especialistas GE em seus quadros.

Em relação às atividades de proteção contra a G Ciber, não são previstos pessoal e equipamentos dessa natureza nos quadros dessas Subunidades. Infere-se assim que há a necessidade de um estudo para atualizar as dotações dessas SU. A atual estrutura de comunicações é deficiente em relação às demandas doutrinárias da AAAe. Não existem meios adequados em quantidade para o correto funcionamento da estrutura sistêmica da AAAe. Em razão disso, está prevista no Projeto Estratégico do Exército Defesa Antiaérea a aquisição de novos equipamentos de comunicações que permitam que o COAAe da Bda AAAe realize as ligações necessárias (Revista Verde Oliva, 2012, p.41).

7.3 AS ATUAIS NECESSIDADES DE LIGAÇÕES DO COAAe DA BRIGADA AAAe

A atividade primordial de um COAAe é receber e difundir informações, o que se faz com o emprego das ferramentas de apoio à decisão. Isso é a grande chave para o funcionamento da DA Ae (BARROSO, 2004, p. 180).

O COAAe P precisa do sistema de vigilância da DAepc para dar início na avaliação das ameaças Ae por parte da AAAe. Sempre que possível, o COAAe P deverá estar justaposto ao OCOAM P, o que facilita muito as ligações entre esses órgãos. A situação onde não é possível tal proximidade torna-se preocupante. Neste caso, para ser alimentado com dados provenientes do OCOAM, o COAAe P ficará dependente dos diversos meios de transmissão a serem apresentados ficando também mais exposto a ataques cibernéticos.

As atuais ligações necessárias do COAAe P nas operações tem sido realizadas conforme o apresentado no quadro 3 (Apêndice A). Nele estão incluídos possíveis meios a serem usados em ligações no futuro. Essas ligações exigem um elevado número de equipamentos de telemática (computadores, switches, antenas, cabos de transmissão, receptores, transmissores, transcodificadores) e softwares de apoio à atividade de C², como sistemas de transmissão e acompanhamento de mensagens.

Ao observar a variedade de sistemas computacionais verifica-se a complexidade das diversas necessidades de ligação do COAAe P. Diante disso pode-se apontar uma séria de novas de exigências.

Será necessário que se efetue a interoperabilidade entre os sistemas computacionais do COAAe P e os sistemas de AAAe das outras Forças Singulares.

Uma forma de obter interoperabilidade e dispor de um servidor de serviços web. Isso permite, por exemplo, a integração com serviços do SC²FTer, o que exige especialistas em TI.

O mesmo deve ocorrer em relação aos sistemas usados pelo SISDABRA. Isso confirma uma condicionante doutrinária contida no manual de campanha C44-8.

> “Os centros de controle da AAAe, em qualquer escalão, devem estar em condições de estabelecer ligações interforças, procurando se beneficiar dos dados e das informações obtidas junto às estruturas de C² com as quais estejam ligados e interagem. Assim, a estrutura de C² da AAAe deverá estar em condições de suportar diferentes protocolos de comunicações e de ligar-se a redes híbridas, interligadas a diversos equipamentos e sistemas de processamento de dados.” (BRASIL, 2013, p. 1-2)

Conforme já exposto no Capítulo 5, o desenvolvimento do RDS é vital para o COAAe P obter interoperabilidade com os demais conjuntos rádio adotados pelo Exército Brasileiro e pela FAB. O RDS (Figura 30) possuirá controle de segurança e criptografia. Por outro lado, é um sistema que exige também conhecimento em desenvolvimento de sistemas computacionais.

Figura 30 – Protótipo de Equipamento RDS

Fonte: Centro Tecnológico do Exército

7.3.1 O COAAe P Baseado no Shelter Orbisat COAAe S-788BR

O EB já dispõe em suas OM de AAAe o COAAe eletrônico desenvolvido no Brasil pela Orbisat em parceria com o Centro Tecnológico do Exército (CTEx). O equipamento opera com a Unidade de Visualização (UV) do Radar SABER M60, podendo operar com o perfil de COAAe S ou de COAAe P. O perfil de COAAe P permite ao usuário visualizar os dados de alvos detectados por mais de um Radar SABER M60, através de conexões em rede com outras unidades com o perfil de COAAe S. A Figura 31 ilustra a rede do COAAe P, a UV mencionada e o equipamento desdobrado utilizando a antena de UHF. A conexão de rede entre as UV são estabelecidas por dispositivos Ethernet convencionais ou por Radio UHF (Harris Falcon III).

Como qualquer rede padrão TCP/IP, esse sistema deve possuir mecanismos de segurança contra G Ciber, o que requer o apoio de especialistas em TI. A integração dessa UV com os outros sistemas da D Aepc também exigirá habilidades em desenvolvimento de software.

Figura 31 - Shelter Orbisat COAAe S-788BR

Fonte: EsACosAAe, modificado pelo autor.

7.4 REFLEXOS DAS NOVAS TECNOLOGIAS NO COAAe DE BRIGADA AAAe

A presença de um sistema AAAe de média altura nas ligações aumenta a relevância do COAAe P como alvo da G Ciber. Esse sistema tem que possuir condições de se ligar diretamente com o COpM, usando protocolos compatíveis com os usados no SISDABRA, e também com o COAAe P. Dessa forma, ficará exposto em dois enlaces distintos de rede, o que exige um cuidado maior quanto à proteção dos sistemas computacionais.

Entende-se que para o COAAe P precisa de maneiras alternativas para se ligar a um COAAe S de AAAe Me Altu e receber dados do mesmo. Na Sequência, a Figura 32 apresenta um exemplo de posto de comando móvel do Sistema Pantsyr S1, sistema de AAAe de Me Altu russo, cuja aquisição está em estudo no Ministério da Defesa.

Figura 32 – Posto de Comando Móvel 9S737MK Ranzhir

Fonte: EsACosAAe

O fato do sistema Pantsyr não ser desenvolvido no Brasil, implica na vulnerabilidade dos russos possuírem as armas cibernéticas específicas para esse material. Assim sendo, será necessário que existam interfaces que façam a integração dados com os sistemas táticos de comunicações existentes no EB como SISCOMIS e também com a EBNet, ou seja, terá que operar em rede, o que exigirá profissionais capacitados para operar tal interface.

A possibilidade de COAAe P ter que se ligar ao OCOAM quando o mesmo estiver embarcado na aeronave E-99 acrescenta novos requisitos de conhecimento em sistemas modernos de telecomunicações e informação dentro da estrutura sistêmica da DA Ae. O E-99 (Figura 33) é um vetor importantíssimo para a manutenção da superioridade aérea. É uma plataforma de alerta antecipado/controle avançado (AEW&C). O acesso do COAAe P ao SISCENDA é visto pela G Ciber como uma porta de acesso aos sistemas daquela aeronave.

Figura 33 – Aeronave E-99

Fonte: Comando de Defesa Aeroespacial Brasileiro

O Radar de Vigilância SABER M200, apresentado na Figura 34, será um sistema definido por software, o que permite que as características básicas do sistema possam ser facilmente reconfiguradas por meio da mudança dos parâmetros em arquivos eletrônicos. Dessa forma, terá alto grau de imunidade eletromagnética, dificultando as ações hostis da GE.

Além disso, o sistema esta sendo desenvolvido pela empresa brasileira EMBRAER Defesa e Segurança em parceria com o CTEx, o que exigirá grande esforço de inteligência para a criação de uma arma cibernética capaz de comprometer o funcionamento do radar. A G Ciber é uma forma de atingir esse sistema radar remotamente. Caberá àqueles que administram o acesso físico e eletrônico ao referido sistema evitar o vazamento de informações úteis para os

desenvolvedores de malwares táticos a exemplo dos que supostamente foram criados nos EUA.

Figura 34 – Radar SABER M200

Fonte: Revista Verde Oliva

7.5 UMA ESTRUTURA DE PROTEÇÃO CIBERNÉTICA PARA COAAe PRINCIPAL

Ao estudar as demandas de C² da AAAe, particularmente no que se refere ao elevado grau informatização requerido por um COAAe de Bda AAAe, é notório que este órgão estará vulnerável diante das ameaças cibernéticas da atualidade. Não criar estruturas para proteger os sistemas de informação e comunicações do COAAe P é admitir o risco do sistema de AAAe acabar destruído ou de ao menos comprometer o controle da nação brasileira sobre seu espaço aéreo. Diante disso, o COAAe requer uma estrutura de G Ciber que lhe ofereça um grau adequado de proteção.

7.5.1 A base de uma proposta de recursos humanos

Em relação à dimensão Humana, observa-se que a necessidade da Bda AAAe venha possuir efetivo para estruturar uma Cia Com, conforme previsto na doutrina de emprego da AAAe. Esta SU poderá possuir especialistas em Op Info defensivas. Isso sugere basicamente duas equipes chefiadas oficiais de carreira: uma voltada para MPE e outra para medidas de proteção Cibernética (MPCiber). Isso de certa forma vai atender a exigência já existente de haver um Oficial de Guerra Eletrônica no EM da Bda AAAe.

Essas equipes devem ser criadas sem depender da criação da Cia Com. Salvo outro juízo, a criação de uma Cia Com seria a proposta ideal. No entanto, outra alternativa é a inserção dessas equipes nos quadros de organização da Bia C, Essas equipes devem ser vinculadas à Seção de Inteligência da Bda AAAe e serem coordenadas pelo E2. A equipe de MPE não é o foco do presente estudo, porém é um elemento relevante na proteção dos sistemas de informação.

A sugestão de uma equipe de proteção cibernética terá como base três especialistas:

1) Um 1º Ten ou Capitão analista de segurança da informação com especialização em Guerra Cibernética realizada no CIGE.

2) Um 2º Sgt técnico e programação de sistemas com especialização em G Ciber conduzida no CIGE; e

3) Um 2º Sgt técnico em redes de computadores com também especializado em G Ciber pelo CIGE.

O analista de segurança da informação pode projetar a estrutura de segurança das redes, incluindo a segurança de equipamentos (acesso físico), dos dados (sistemas de autenticação) e de sistemas operacionais de servidores. A ele cabe implementar e monitorar a política de segurança da informação. Essa especialização tem como requisito o profundo conhecimento do protocolo TCP/IP e dos sistemas operacionais. Exige-se que o analista de segurança também tenha domínio sobre linguagens de programação. O mesmo deve possuir conhecimento de configuração e atualização de regras em firewalls, conhecimento de protocolos de interoperabilidade entre redes. Além disso, é capaz de monitorar tráfego de rede e operar sistemas de detecção de intrusão. Em resumo, pode ser considerado um hacker de proteção. Este especialista realiza análises de riscos, auditorias em SI e planeja contingências e recuperação em sinistros (BRASIL, 2015e).

O técnico em programação pode desenvolver e interpretar algoritmos de sistemas; pode criar e manipular bases de dados, ler e interpretar códigos em diversas linguagens de programação e modelagem de dados. Pode desenvolver e customizar aplicações para navegadores de redes e sistemas operacionais, atendendo às orientações do Manual Técnico para Metodologia de Desenvolvimento de Software do Exército, EB80-MT-78.001.

O técnico em redes instala e configura dispositivos de comunicação digital e programas em equipamentos de rede. Pode executar diagnóstico e corrige falhas em

redes de computadores. Instala e mantém cabeamentos de redes. Configura acessos de usuários. Configura serviços de rede, tais como firewall, servidores web e correio eletrônico. Pode também implementar recursos de segurança em redes de computadores (BRASIL, 2015f).

Muitas GU do EB já possuem informalmente equipes de TI compostas por militares que possuem parcela dessas competências, porém não trabalham voltados especificamente paras as medidas de G Ciber.

Essas especializações ora propostas estão disponíveis nos estabelecimentos de ensino nacionais e no exterior. As capacidades mencionadas permitem o uso adequado das diversas ferramentas disponíveis a serem sugeridas para as dimensões lógica e física. Serão capazes de apresentar soluções nas diversas situações em que for necessário integrar sistemas de comando e controle conforme se verifica no Apêndice A. As diversas formas de estabelecer comunicações Além disso, podem adotar com maior facilidade as normas ABNT NBR ISO/IEC 27001, NBR ISO/IEC 27002 e NBR ISO/IEC 27005, que estabelecem requisitos e boas práticas para implementação de Sistema de Gestão de Segurança da Informação (SGSI), técnicas para gestão da segurança da informação e gestão de riscos em sistemas de informação, respectivamente. Em particular, a norma ABNT NBR ISO/IEC 27002 (Técnicas de Segurança – Código de prática para a gestão da segurança da Informação) prevê 11 controles de segurança da informação que envolvem 39 categorias principais de segurança (FRIEDRICH, 2014 ,p.19).

Caberá também a esta equipe, possuir um canal técnico com os Dst de G Ciber dos escalões superiores, uma vez que possuirá conhecimento para implementar as recomendações recebidas desses órgãos.

A seleção de talentos para comporem esta equipe pode seguir alguns requisitos. O oficial poderá ser oriundo do Instituto Militar de Engenharia, caso outro estudo mais aprofundado revele esta necessidade. Em relação aos praças, propõe-se que o técnico em redes pode ser da arma de comunicações e é desejável que o técnico em programação seja também especialista em AAAe. Isso deverá levantado no âmbito do EB ou mediante a obtenção de matrículas em cursos disponíveis nos diversos estabelecimentos de ensino. Toda a equipe deve ser selecionada e especializada mediante os critérios do Sistema de Inteligência do Exército.

7.5.2 A base de uma proposta de recursos tecnológicos

Os recursos tecnológicos para a estrutura de G Ciber para a proteção do COAAe de Bda AAAe estão entre as soluções apresentadas no Capítulo 6. Merecem destaque as técnicas aplicadas a Firewall, o dispositivo UTM e o Antivírus Corporativo (AV BR).

É importante saber que qualquer solução de segurança baseada em software ou hardware exige o acompanhamento e homologação dos órgãos que coordenam essas soluções no âmbito do EB. São esses órgãos: o CDS, o CITEx e o CDCiber.
No caso das soluções que afetem as ligações com órgãos da FAB, é necessário observar as recomendações do COMDABRA. Logo, as soluções desenvolvidas pela Eqp de Medidas de Proteção Cibernética (MPCiber) devem seguir as recomendações desses canais técnicos para os sistemas sejam desenvolvidos com o mínimo de falhas de segurança em seus códigos. Os documentos reguladores são a Diretriz para Utilização e Gestão de Software no Exército Brasileiro (GESOFT) e as Instruções Reguladoras Sobre Segurança da Informação nas Redes de Comunicação e de Computadores do Exército Brasileiro (IRESER).

Grande parcela das soluções de proteção cibernética podem vir incorporadas nos materiais e sistemas providos pelo EB e pela FAB. Neste caso, caberá à equipe de MPCiber apresentar soluções complementares para aumentar a proteção ou eliminar alguma vulnerabilidade.

Uma solução que pode existir na estrutura de C² da Bda AAAe é o UTM (Unified Threat Management). Essa solução reúne diversas funções de segurança em um único equipamento. Integra por exemplo firewall, detector de intrusão, antivírus, VPN, filtro de conteúdo (Proxy) e balanceamento de carga. Além disso, memoriza e gera relatórios sobre todo o funcionamento da rede.

O sistema de comunicações Rádio devera operar com RDS compatíveis com a arquitetura SCA e formas de ondas desenvolvidas pelas Forças Armadas Brasileiras. Esses Eqp devem permitir a inserção de algoritmos proprietários do Exército Brasileiro para criptografar e decriptografar, de forma automática, as informações transmitidas.

Todos os sistemas de C² devem possuir microcomputadores portáteis próprios em quantidade redundante. Isso evita o uso improvisado de equipamentos estranhos

aos sistemas. Esses microcomputadores não podem ter acesso livre para aos conectores USB e devem possuir Antivírus homologado no EB.

Todos os sistemas computacionais devem possuir acesso mediante autenticação.

A estrutura deverá possuir equipamentos possibilitem redundância aos sistemas. Neste caso as redes ad hoc podem ser uma das alternativas. Além disso, essas redes devem ser segmentadas.

A Bda AAAe deve possuir geração própria de energia capaz de manter todos os sistemas alimentados por longos períodos no TO ou na ZI.

Em relação às dependências em campanha é importante que o pessoal de G Ciber atuem e se alojem em ambientes reservados. Essa é uma forma de preservar esses especialistas e seus pertences para que fiquem fora do alcance e da observação de elementos a serviço de operações de informação adversas. Os equipamentos críticos e seus manuais técnicos também devem estar em ambientes de acesso restrito, protegidos por biometria, cofres e outras restrições de acesso.

Todos os documentos técnicos e de operação dos equipamentos de críticos que estejam em formato digital devem ser criptografados. Para isso, é necessário que exista um sistema de criptografia homologado no EB. Os documentos de treinamento devem ser fornecidos em extratos, segmentando as informações de forma atender os usuários na medida adequada para cada elemento.

Quanto à estrutura de treinamento, a Bda AAAe precisa dispor de um simulador de incidentes cibernéticos que podem ocorrer em um COAAe P. Caso não seja possível que este simulador fique nas instalações da Bda AAAe, esta deve possuir acesso ao mesmo por meio do órgão que o possua. Para isso, se propõe que exista um simulador específico para o perfil de tratamento de incidentes que envolvem a DA Ae.

7.6 CONSIDERAÇÕES

Encerrando o presente capítulo, infere-se que foi necessário apresentar sugestões básicas para que exista uma estrutura de G Ciber na Bda AAAe que proporcione proteção ao seu COAAe. Tal proposta teve embasamento no estudo das demandas do COAAe P e também no estudo dos demais aspectos das doutrinas de C² e de G Ciber apresentados nos capítulos anteriores.

8. CONCLUSÃO

O presente trabalho buscou avaliar a necessidade de apresentar bases para a elaboração de uma proposta de estrutura de guerra cibernética para a proteção do centro de operações de uma Brigada de Artilharia Antiaérea.

Para isso, no Capítulo 1, foram apresentados os argumentos que motivaram o estudo desse tema e os métodos de pesquisa. Foram definidos os objetivos e a suposição a serem analisados com base nos fundamentos doutrinários e na avaliação dedutiva dos aspectos a serem estudados.

A metodologia científica adotada foi descrita no Capítulo 2, no qual constam os procedimentos técnicos adotados durante a realização do trabalho.

No Capítulo 3 foram estudados os aspectos doutrinários da Guerra Cibernética. Entre os aspectos estudados, observou-se que, no nível tático de decisão, as ações de G Ciber possuem permeabilidade em todos os domínios operacionais onde atuam as defesas antiaéreas. Assim, pode-se afirmar que a AAAe está no alcance dessas ações. Verificou-se que, conforme o princípio do efeito, a G Ciber prioriza suas ações com base no resultado efetivo. Assim, quanto mais vulnerável e compensador for o alvo, maior será o efeito e a prioridade de ataque. Se os sistemas de C² da AAAe não estiverem protegidos serão alvos prioritários da G Ciber.

A Doutrina de Op Info revela que o planejamento da G Ciber é apoiado por meios de inteligência, podendo levantar dados sobre as redes do oponente. Assim se observa a importância do sigilo no que se refere aos sistemas de informação, revelando a necessidade uma estrutura de segurança. De acordo com a doutrina vigente, uma Célula de Operações de Informação pode planejar um ataque cibernético sincronizado com medidas de ataque eletrônico, precedendo uma manobra convencional. Da mesma forma, essa ação preliminar pode ser feita em favor do sucesso de um ataque aéreo que necessite que uma defesa AAe seja neutralizada. Do exposto, infere-se que os que se faz necessário estudar mudanças na atual estrutura de Comando e Controle da Bda AAAe do Exército Brasileiro.

Com a finalidade de subsidiar a pesquisa, no Capítulo 4 estudou-se a doutrina vigente de comando e controle e os reflexos da mesma na proteção de uma Bda AAAe. Entre os atuais aspectos doutrinários de C² abordados, observa-se que a preservação do domínio da informação implica em medidas de proteção. Assim, ao conceber um sistema de C², deve-se prever a segurança do mesmo, mediante

criteriosa seleção de pessoal e equipamentos. Para se adequar a uma mudança de ambiente por causa de ações de G Ciber, o COAAe P deve incorporar inovações tecnológicas e ser reestruturado quando necessário.

Para obter uma significativa melhora na capacidade de observar, orientar-se, decidir e agir se faz necessário adotar o conceito de GCR. A formação da consciência situacional na atualidade exige o funcionamento ininterrupto dos recursos de C², particularmente para permitir tomadas de decisão oportunas diante das ameaças aéreas. A velocidade da tomada de decisão depende da dinâmica do Ciclo de Boyd. Logo, o ciclo deve ficar isento de interferências hostis.

Verificou-se que a GCR é estruturada em tecnologia da informação. Portanto, as ações de Guerra Cibernética podem reduzir consideravelmente o poder de combate de uma força que aplica este conceito. Isso exige a adoção de novas tecnologias e mudanças estruturais.

Verificou-se que o SISMC² pode oferecer diversos serviços seguros para o exercício do comando e controle. Observou-se que é possível que um COAAe P se apoie na estrutura do SISMC² desde que sejam respeitadas normas de segurança específicas. Conclui-se então que pode ser necessário inserir medidas de proteção na estrutura de comando e controle da AAAe, o que exige operadores capacitados em sistemas software, telecomunicações e enlace de dados.

Verificou-se também a Artilharia Antiaérea deverá estar com seus sistemas informatizados e integrados ao SISDABRA por meio de um Centro de Operações Antiaéreas Eletrônico de Brigada. Esse material pode exigir uma interface com o OCOAM por meio de uma rede, o que indica a necessidade de possíveis alterações na atual estrutura de Comando e Controle da Bda AAAe do Exército Brasileiro.

Diante do conjunto de informações apresentadas no capítulo 5 verificou-se a necessidade do COAAe P possuir interfaces de comunicações suficientes para transmitir e receber dados e voz via SISCOMIS, particularmente na Amazônia, pois existem restrições para os rádios transmitirem dados na faixa de HF.

O COAAe P deverá estar apto a se conectar a EBNET, pois essa rede oferece a possibilidade integração com às demais redes das Forças Armadas e comunicação com COAAe S remotos, o que exige especialistas em TI.

Como o SISCOMIS, a EBNET e as Redes de Controle do Espaço Aéreo operam com serviços contratados junto a operadoras civis de telecomunicações,

conclui-se que é preciso profissionais e mecanismos que monitorem essas redes contra ameaças cibernéticas.

Observou-se que a aeronave E-99 é elo vital do SISCENDA e um dos vetores mais importantes do SISDABRA, sendo assim um alvo prioritário da G Ciber. Se o COAAe P não possuir proteção, o mesmo poderá ser uma porta de acesso ao E-99.

.Em curtas distâncias, o rádio continua a ser protagonista entre os sistemas que devem compor o COAAe P, particularmente na ligação com os COAAe S. O COAAe. O sistema rádio deverá ser interoperável, sendo capaz de transmitir e receber dados e voz, e empregando plataformas e protocolos compatíveis com os sistemas de controle do espaço aéreo utilizados pela FAB.

Em relação à tecnologia a ser incorporada nos futuros materiais de AAAe, estudos apontam para a tendência de utilização de rádios definidos por software (RDS), trazendo portabilidade de formas de onda e interoperabilidade entre as diferentes Forças. O RDS é uma solução que vai ao encontro dos requisitos de segurança para fazer frente a ameaças cibernéticas, pois incorporas criptogramas. Assim, conclui-se que isso vai exigir operadores dotados de novas capacidades.

Quanto aos meios das telefonias privadas e da Internet, verificou-se que esses meios podem ser usados se necessário. São recursos que carecem de rigorosas normas de Segurança da Informação, ou seja, necessitam possuir proteção contra G Ciber. Assim, a complexidade e a variedade dos meios de C^2 disponíveis para o estabelecimento de enlaces no COAAe P revelam a necessidade de possíveis alterações na atual estrutura de Comando e Controle da Bda AAAe do Exército Brasileiro, o que vai exigir especialistas em telecomunicações, em redes de computadores e em segurança da Informação.

Ao estudar o capítulo 6, verificou-se que existe uma grande variedade ferramentas e atores capazes de realizar ações de G Ciber hostis. As ações podem partir de outros continentes ou mesmo do espaço cibernético brasileiro, o qual se encontra favorável à ação de hackers. O estudo possibilitou a identificação das ameaças empregadas na Guerra Cibernética capazes atuar diretamente nos meios de comando e controle de um centro de comando e controle de uma Bda AAAe.

Confirmou-se que os meios da defesa aeroespacial estão entre os alvos prioritários nas campanhas aérea e cibernética do inimigo, sendo alvos também da inteligência e da GE.

Observou-se a necessidade de meios próprios de geração de energia elétrica aos sistemas de C² devido aos ataques cibernéticos contra empresas geradoras e fornecedoras de eletricidade.

Diante da assertiva de que um Hacker pode neutralizar outro Hacker, conclui-se sobre a prioridade que deve ser dada na formação e identificação de talentos em cibernética, pois estes especialistas são capazes de desenvolver, integrar e proteger sistemas de comunicações centrados em redes. Verificou-se que uma forma de combater um ator cibernético ameaçador é fazê-lo desistir do ataque. Assim, é importante identificar o perfil dos recursos humanos e as opções de material de comunicações e de TI que podem ser adotados na estrutura de G Ciber na proteção de um COAAe principal.

Pode-se concluir que a complexidade dos meios e técnicas de proteção dos meios informatizados de um COAAe P revelaram a necessidade de haver mudanças na atual estrutura de comando e controle da Bda AAAe do Exército Brasileiro.

Encerrando o presente trabalho, infere-se que será necessário apresentar soluções que sirvam de subsídios para a formulação de uma proposta de estrutura de G Ciber na Bda AAAe que proporcione proteção ao COAAe P. Essa conclusão confirma também a hipótese formulada no capítulo 1. Considerando a dificuldade do Dst Cj G Ciber dedicar apoio exclusivo à AAAe, as sugestões apresentadas no capítulo 7 representam a utilidade da pesquisa ora realizada, pois vários aspectos abordados revelaram claramente a necessidade do COAAe da Bda AAAe possuir proteção contra guerra cibernética em suas próprias estruturas, baseadas principalmente na dimensão humana.

Além de atender os objetivos específicos traçados para a pesquisa no capítulo 1, o presente trabalho poderá servir para o levantamento de novos requisitos a serem incluídos nos projetos de modernização dos sistemas de C² da Bda AAAe e também servir de apoio numa futura atualização do manual de campanha C44-8, Comando e Controle na Artilharia Antiaérea.

Por fim, ao estudar as demandas de C² da AAAe, particularmente no que se refere ao elevado grau informatização requerido por um COAAe de Bda AAAe, é notório que este órgão estará vulnerável diante das ameaças cibernéticas da atualidade. Ao deixar de criar estruturas para proteger os sistemas de informação e comunicações do COAAe P pode-se admitir o risco do sistema de AAAe acabar

destruído ou talvez comprometer o controle da nação brasileira sobre seu espaço aéreo. Diante disso, o COAAe requer uma estrutura de G Ciber que lhe ofereça um grau adequado de proteção.

_____

HAROLDO **HEITOR** DE CARVALHO – Maj Art

REFERÊNCIAS

ALVES, Sidney César Coelho. **Estudo Conceitual dos Principais Sistemas de Enlace de Dados Táticos Atualmente em Uso no Mundo.** 2003. 46 f. Trabalho Individual (Curso de Especialização em Análise do Ambiente Eletromagnético). Instituto Tecnológico de Aeronáutica, São José dos Campos, 2003.

ALMADA, Eduardo Miguel Arrúa. **Guerra Cibernética: Métodos de ataque e defesa**. 2013. 51 f. Trabalho de Conclusão de Curso (Altos Estudos Militares) – Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2013.

APRSBRASIL. **Rádio Definido por Software.** Disponível em: < http://www.aprsbrasil.com/sdr_softwaredefinedradios.html>. Acesso em: 12 fev. 2015.

BARROSO, João Marcio Pavão. **A estrutura de comando e controle da artilharia antiaérea no contexto do SISDABRA: uma nova concepção.** 2004. Dissertação (Mestrado em Ciências Militares)-Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2004.

BASTOS, Ezequiel da Silva. **Avaliação do emprego permanente do satélite nas comunicações táticas de brigada do Exército Brasileiro.** 2012. 56 f. Trabalho de Conclusão de Curso (Curso de Aperfeiçoamento Militar) - Escola de Aperfeiçoamento de Oficiais, Rio de Janeiro, 2012.

BRASIL. Comando da Aeronáutica. **DCA 1-1: Doutrina Básica da Força Aérea Brasileira.** 1. Ed. Brasília, DF, 2005.

_____. Comando da Aeronáutica. Departamento de Controle do Espaço Aéreo. **DCA 102-1, Requisitos Básicos das Redes de Comunicações do COMAER .** 2. Ed. Brasília, DF, 2011.

_____. Comando da Aeronáutica. Estado Maior da Aeronáutica. Ofício nº 3/6SC1,. Brasília, 15 abr. 2004.

_____. Exército. Centro de Comunicações e Guerra Eletrônica**. Empresa brasileira Lança antivírus 100% nacional.** Disponível em: <http://www.ccomgex.eb.mil.br/index.php/pt_br/78-inicio/71-empresa-brasileira-lanca-antivirus-100-nacional>. Acesso em: 30 jan. 2015

_____. Exército. Centro de Comunicações e Guerra Eletrônica. **Programa C2 em Combate.** Disponível em: < http://www.ccomgex.eb.mil.br/ cige/sent_colina/5_edicao_ago_07/conteudo/Pdf/ARTIGO%20C2%20EM%20COMBATE%20-%20Sentinela%20(2).pdf**>.** Acesso em 10 fev. 2015a.

_____. Exército. Centro de Desenvolvimento de Sistemas. Termo de Referência nº 02 SSI/DSI. Aquisição de Solução Corporativa de Antivírus Multiplataforma com Gerência Centralizada. Brasília-DF, 7 nov. 2014.

_____. Exército. Centro Tecnológico. **Rádio Definido por Software (RDS).** Disponível em: < http://www.ctex.eb.br/index.php/component/content/article/11-pad/projetos/149-rds-radio-definido-por-software>. Acesso em 20 fev. 2015b.

_____. Exército. Centro Tecnológico. **Radar SABER M200.** Disponível em: < http://www.ctex.eb.br/index.php/component/content/article/11-pad/projetos/147-radar-saber-m200>. Acesso em 20 fev. 2015c.

_____. Exército. Estado-Maior. **Bases para a Transformação da Doutrina Militar Terrestre.** 1. Ed**.** Brasília, DF, 2013.

_____. Exército. Escola de Artilharia de Costa e Antiaérea. **EB 60 – ME – 23.021: Manual de Ensino do Centro de Operações Antiaéreas - Estabelecimento e Operação do Centro de Operações Antiaéreas.** 1. Ed**.** Rio de Janeiro, RJ, 2013a.

_____. Exército. Escola de Artilharia de Costa e Antiaérea. **O emprego da Artilharia Antiaérea e a necessidade de coordenação do espaço aéreo**. In: SIMPÓSIO DE COORDENAÇÃO DO ESPAÇO AÉREO, 1., Rio de Janeiro, 2011. EsACosAAe, 2011b.

_____. Exército. Escola de Comando e Estado-Maior: **ME 21 -253: Formatação de trabalhos acadêmicos, dissertações e teses**. 2. ed. Rio de Janeiro, 2007.

_____. Exército. Estado-Maior. **C 11-1: Emprego das Comunicações.** 2. Ed**.** Brasília, DF, 1997.

_____. Exército. Estado-Maior. **C 11-30: As Comunicações na Brigada.** 2. Ed. Brasília, DF, 1998.

_____. Exército, Estado-Maior. **C 44-1: Emprego da artilharia antiaérea.** 2. Ed. Brasília, DF, 2001.

_____. Exército. Estado-Maior. **C 44-8: Comando e controle na artilharia antiaérea.** 1. Ed. Brasília, DF, 2003.

_____. Exército. Estado-Maior. **EB20-MF-10.102: Doutrina militar terrestre**. 1. Ed. Brasília, DF, 2014.

_____. Exército. Estado-Maior. **EB20-MF-10.103: Operações**. 1. Ed. Brasília, DF, 2014a.

_____. Exército. Estado-Maior. **EB20-MC-10.213: Operações de informação.** 1. Ed. Brasília, DF, 2014b.

_____. Exército. Estado-Maior. **EB20-MC-10.202: Força terrestre componente .** 1. Ed. Brasília, DF, 2014c.

_____. Exército. Estado-Maior. **EB20-MC-10.301: Força terrestre componente nas operações.** 1. Ed. Brasília, DF, 2014d.

_____. Exército. Portaria nº 351, Comandante do Exército, de 20 de maio de 2013. Transforma a 1ª Companhia de Guerra Eletrônica em 1º Batalhão de Guerra Eletrônica e dá outras providências. **Boletim do Exército**, Brasília, DF, n. 21, p. 15, 24 maio 2013.

_____. Ministério da Defesa, **Estratégia Nacional de Defesa**. Brasília, DF, 2008.

_____. Ministério da Defesa. Estado-Maior. **MD 31 -D-03 Doutrina Militar de Comando e Controle.** 1 a Ed. Brasília, DF: 2006

_____. Ministério da Defesa. Estado-Maior. **MD 31 -M-07 Doutrina Militar de Defesa Cibernética.** 1 a Ed. Brasília, DF: 2014e.

_____. Ministério da Defesa. Estado-Maior. **MD35-G-01, Glossário das Forças Armadas**. 1. Ed. Brasília, DF: 2007.

_____. Ministério da Defesa. Estado-Maior. **MD30-M-01, Doutrina de Operações Conjuntas**. Vol 1. 1. Ed. Brasília, DF: 2011a.

_____. Portal Brasil. **Novo sistema de controle aéreo começa a operar em Brasília.** jan, 2012. Disponível em: <http://www.brasil.gov.br/defesa-e-seguranca/2012/01/novo-sistema-de-controle-aereo-comeca-a-operar-em-brasilia>. Acesso em 20 fev. 2015d.

_____.Ministério da Educação. **Catálogo Nacional dos Cursos Superiores de Tecnologia.** Disponível em: < http://portal.mec.gov.br/index.php?Itemid=719>. Acesso em: 02 mar. 2015e.

_____.Ministério da Educação. **Catálogo Nacional de Cursos Técnicos.** Disponível em: < http://pronatec.mec.gov.br/cnct/et_informacao_comunicacao/ et_informacao_comunicacao.php >. Acesso em: 02 mar. 2015f.

BLUEPEX. **Unified Threat Management**. Disponível em: <http://www.bluepex.com/utm.php>. Acesso em: 23 fev. 2015.

BUSCHER, Alexandre Serio. **Emprego de Comunicações com Equipamentos Baseados em Software num Grupo de Artilharia Antiaérea de Divisão de Exército.** Informativo Antiaéreo Rio de Janeiro, nº 8, p. 61-69, 2013.

CANONGIA, Claudia; MANDARINO JUNIOR, Raphael. **Segurança cibernética: o desafio da nova sociedade da informação**. Parceria Estratégica. Brasília-DF. v. 14 . n. 29. p. 21-46. jul-dez 2009.

CARNEIRO, João Marinonio Enke. **A Guerra Cibernética: uma proposta de elementos para formulação doutrinária no Exército Brasileiro**. 2012. 203 f. Tese (Doutorado) – Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2012.

Centro Tecnológico do Exército. Revista Verde Oliva, Brasília, n.223, p. 24-25, abr. 2014.

CERT.br. Comitê Gestor da Internet no Brasil. **Estatísticas dos Incidentes Reportados.** 2013. Disponível em: <http://www.cert.br/stats/incidentes/>. Acesso em: 20 fev. 2015.

CORREA, Fernanda das Graças. **Pela defesa do espaço cibernético brasileiro: panorama mundial e nacional.** 27 fev. 2013. Disponível em: < http://www.defesanet.com.br/cyberwar/noticia/9860/>. Acesso em: 20 fev. 2015.

Defesa cibernética descomplicada. Revista Verde Oliva, Brasília, n.223, p. 40-42, abr. 2014.

ESTADOS UNIDOS DA AMÉRICA. Congressional Research Service. **Report for Congress.** Washington, DC, 2001.

FINK, Kallie D. et al. **Considerações para as operações cibernéticas ofensivas.** Military Review, Fort Leavenworth, v. 69, nº. 5, p.38-46, set.-dez. 2014.

FONTENELE, Marcelo Paiva. **Análise e proposta de articulação de esforços nocontexto da defesa cibernética da administração pública federal**. 2008. 65 f. Trabalho de Conclusão de Curso – Universidade de Brasília, Brasília, 2008.

_____. Marcelo Paiva. **Proposta de Estruturação do Sistema de Guerra Cibernética no Âmbito das Forças Armadas**. Centro Integrado de Guerra Eletrônica. Brasília, DF, 2007. 7 f.

FRIEDRICH, Lucimara Dalla Porta Menezes. **Um sistema Web para Análise e gestão da segurança da informação segundo a Norma ABNT NBR ISO IEC 27002**. 2014. 73 f. Trabalho de Conclusão de Curso (Curso Superior de Tecnologia em Redes de Computadores) - Universidade Federal de Santa Maria, Santa Maria, RS, 2014.

GIL, Antônio Carlos. **Como elaborar projetos de pesquisa**. 4. Ed. São Paulo: Editora Atlas, 2002.

GOMES, Hélio. **Cyberterror no Espaço.** Revista Istoé. nº 2210. p. 114. mar. 2012.

LAKATOS, E. M.; MARCONI, M. A. **Metodologia Científica.** 5. Ed. São Paulo: Editora Atlas, 1991.

MANDARINO JUNIOR. Raphael. **Segurança e defesa do espaço cibernético brasileiro.** 1. ed. Recife: Cubzac, 2010. 182p.

_____. Raphael . **Entrevista de Mariana Lucena sobre Segurança Cibernética.** In: Revista Galileu. 26 jun. 2009. Disponível em: <http://dsic.planalto.gov.br/ noticias/65-entrevista-do-diretor-do-dsic-a-revista-galileu>. Acesso em: 02 set. 2014.

_____. , Raphael. **Um estudo sobre a segurança e a defesa do espaço cibernético brasileiro**. 2009. 156 f. Monografia de Especialização. Universidade de Brasília, Brasília, 2009.

MENDONÇA, Evaldo Galvão. **Bridge Firewall – Uma Solução Baseada em software livre para a Segurança da EBNET**. Salvador, BA, 2007, 10p.

MICROSOFT CORPORATION. **O que é um Firewall.** Disponível em: <http://windows.microsoft.com/pt-br/windows/what-is-firewall#1TC=windows-7>.Acesso em: 12 fev. 2015.

MORESI, Eduardo Amadeu Dutra. **Informação: uma arma cibernética?** Universidade Católica de Brasília, Brasília, DF, 2011? 6 f.

NATIONAL INSTRUMENTS CORPORATION. **Universal Software Radio Peripheral.** Disponível em: < http://www.ni.com/rf/pt/>. Acesso em: 12 fev. 2015.

O GLOBO. **Novo vírus Gauss rouba dados de banco no Oriente Médio.** 10 ago. 2012. Disponível em: < http://oglobo.globo.com/sociedade/tecnologia/novo-virus-gauss-rouba-dados-de-bancos-no-oriente-medio-5743732> . Acesso em: 20 jan. 15.

PAIVA JUNIOR, Nilson Maciel et al. **Introdução ao Desenvolvimento de Rádios Definidos por Software para Aplicações de Defesa**. In: XXX SIMPÓSIO BRASILEIRO DE TELECOMUNICAÇÕES, 5. Brasília 2012. Rio de Janeiro: Instituto Militar de Engenharia, 2012.

PASINI, Paulo César. **A Guerra Cibernética e as Operações de Informação no Nível Operacional.** 2012. 106 f. Trabalho de Conclusão de Curso (Altos Estudos Militares) – Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2012.

PINHEIRO, Alvaro de Souza. **A Tecnologia da Informação e a Ameaça Cibernética na Guerra Irregular do Século XXI**. PADECEME, Rio de Janeiro, n° 18, p. 4-11, 2° quadrimestre. 2008

PINTO, Marcelo Luis Seabra. **Guerra cibernética na MB: desafios e perspectivas para a próxima década**. 2009. 46 f. Monografia (Curso de Política e Estratégia Marítimas) – Escola de Guerra Naval, Rio de Janeiro, 2009.

ROHR, Altieres. **Vírus 'Flame' foi desenvolvido pelos Estados Unidos e Israel, diz jornal.** 20 jun. 2012. Disponível em: < http://g1.globo.com/tecnologia/noticia/2012/06/virus-flame-foi-desenvolvido-pelos-estados-unidos-e-israel-diz-jornal.html > . Acesso em: 20 jan. 15.

SENADO FEDERAL. **Segurança cibernética e soberania nacional**. Audiência Pública. Brasília, DF, 6 dez. 2013.

SHAKARIAN, Paulo, **Análise da Campanha cibernética da Rússia contra a Geórgia em 2008**. . Military Review, Fort Leavenworth, p.68-73, nov-dez. 2011

SILVA, Wellington Guilherme da . **Laboratório de Simulação de NCW (Network Centric Warfare)**. Instituto Tecnológico da Aeronáutica. São José dos Campos, SP, 2007. 5p.

SYMANTEC CORPORATION. **O Duqu: Precursor de um próximo Stuxnet.** Disponível em: < http://www.symantec.com/pt/br/outbreak/?id=stuxnet >. Acesso em: 12 jan. 2015.

THEILER, Olaf. **Novas ameaças: a dimensão cibernética**. Revista da Nato. Disponível em: < http://www.nato.int/docu/review/2011/11-september/Cyber-Threads/PT/index.htm>. Acesso em: 20 jan. 15.

VOZ DA AMÉRICA. **EUA: 500 milhões de dólares para fabrico de ciberarmas.** Disponível em: <www.voaportugues.com/content/article-03-21-12-pentagon-cyberwars-143653646/1450967.html>. Acesso em: 20 fev. 2015.

APÊNDICE A

Quadro 3 – Ligações a serem realizas por um COAAe Principal

Ligação do COAAe P	Resp p/ ligação	Finalidade	Meios de transmissão	Eqp e Sis de infomação	Eqp e Sis de apoio à decisão	Tipo de Informação	Meios Altn
COAAe S AAAe Bx Altu	Cmdo Bda AAAe	1. Acn da DA Ae;, 2. Difusão de MCCEA e MCCAAe; 3. Coordenação; 4. Controle; 5. Difusão de alerta.	1. Rádio VHF/UHF; 2. Satélite; 3. Redes TCP/IP (Ethernet); e 4. Op de Telecom.	1. RDS (1); 2. Harris Falcon III; 3. EBNET; e 4. SISCOMIS (2)	1. COAAe Elt - Bia AAAe/ GAAAe (3) 2. Unidade de visualização Rdr SABER M60 (4).	1.Dados; 2. Imagens; e 3. Voz (5).	1. Internet(6); e 2. RDS HF (1).
COAAe S AAAe Me Altu	Cmdo Bda AAAe	1. Acn da DA Ae (sfc); 2. Difusão de MCCEA e MCCAAe 3. Coordenação; 4. Controle; e 5. Difusão de alerta.	1. Rádio VHF/UHF; 2. Satélite; 3. Redes TCP/IP (Ethernet); e 4. Op de Telecom.	Posto de Cmdo Móvel 9S737MK Ranzhir (7).	Em estudo	1.Dados; 2. Imagens; e 3. Voz (5).	Em estudo
COpM /CCOA OCOAM P / ELAAe	COMDABRA ou Cmdo da FAC	1.Acn das DA Ae; 2. Difusão de MCCEA e MCCAAe 3. Coordenação; 4. Controle; 5. Difusão de alerta; e 6. Visualização da SAGDA.	1. ANT (8); e 2. Redes TCP/IP (Ethernet).	1. DACOM; 2. SISCENDA; 3. Intraer (9); e 4. TF 1,2,e 4 (10)	1. Sagitário; 2. X4000 (11); e 3. SISTRASAG (12)	1.Dados; 2. Imagens; e 3. Voz (5).	SISCOMIS
CC Op – FTC Célula Funcional Proteção / EDAAe	Cmdo FTC	1.Acomp da Man da FTC. 2. Difusão de MCCEA MCCAAe 3. Coordenação; 4. Controle; 5. Difusão de alerta; 6. Ligação com o EDAAe; 7. Videoconferência; 8. Mdd de proteção e autodefesa; e 9. Alerta Cibernético (13)	1. SISTAC; 2. Redes TCP/IP (Ethernet); e 3. Satélite.	1. Modo de Telemática de integração CII (1); e 2. SISCOMIS; 3. RDS (1); e 4. EBNET	Sistema C2 Cmb (1)	1.Dados; 2. Imagens; e 3. Voz (5).	Outros meios do SISMC2
Sensores de Vigilância da Bda AAAe	Cmdo Bda AAAe	1. Difusão de alerta; 2. Compartilhamento da síntese radar; e 3. Difusão de IFF.	1. Rádio VHF/UHF; 2. Satélite; e 3. Redes TCP/IP (Ethernet)	RDS (1)	Rdr SABER M200 (1)	1.Dados; 2. Imagens; e 3. Voz (5).	Em Estudo
COAAe S da FAB (GAAAD)	Cmdo da Bda AAAe	1. Acn da DA Ae;, 2. Difusão de MCCEA e MCCAAe; 3. Coordenação; 4. Controle; 5. Difusão de alerta.	1. ANT (8); 2. Redes TCP/IP (Ethernet); e 3. Rádio VHF/UHF	1. DACOM; 2. SISCENDA; 3. RDS (1) 4. Intraer (9); e 5. TF 1,2,e 4 (10)	1. Sagitário; 2. Unidade de visualização Rdr SABER M60 (4); e 3. ETT (sfc).	1.Dados; 2. Imagens; e 3. Voz (5).	SISCOMIS
COAAe P de outra Bda AAAe	Cmdo Bda AAAe (Sit à Es)	1. Integração de Sis Ct Alr AAAe; 2. Mdd Coor; e 3.Difusão de alerta.	1. Rádio VHF/UHF; 2. Satélite; 3. Redes TCP/IP (Ethernet); e 4. Op de Telecom.	1. RDS (1); 2. Harris Falcon III; 3. EBNET; e 4. SISCOMIS (2)	1. COAAe Elt - Bia AAAe/ GAAAe (3) 2. Unidade de visualização Rdr SABER M60 (4).	1.Dados; 2. Imagens; e 3. Voz (5).	1. Internet (6); e 2. RDS HF (1).
OCOAM (embarcado) (14)	COMDABRA ou Cmdo da FAC	1.Acn das DA Ae; 2. Difusão de MCCEA e MCCAAe 3. Controle; 4. Difusão de alerta; e 5 Vis da SAGDA.	1. ANT(8); e 2. Redes TCP/IP (Ethernet).	SISCENDA	1.Sagitário; e 2. X4000 (11).	1.Dados; 2. Imagens; e 3. Voz (5).	Em estudo

LEGENDA:
(1) Em desenvolvimento.
(2) Para longas distâncias, podendo utilizar ETT (sfc).
(3) Shelter Orbisat COAAe S-788BR.
(4) Perfil COAAe P.
(5) Mediante criptografia e criptografia.
(6) Acesso à EBNET via VPN.
(7) Pertence ao Sistema AAAe Pantsyr S1.
(8) Sistema Telesat / Rede de Telecomunicações da Aeronáutica.
(9) Rede corporativa da FAB.
(10) Rede telefônica privativa da FAB.
(11) Em fase de substituição.
(12) Meio alternativo de visualização da SAGDA.
(13) Por intermédio do Dst de G Ciber e da Célula Funcional Op Info.
(14) OCOAM S embarcado em aeronave E-99.

Fonte: o autor